

医院电子病历 数字签名实施指南

编 著 中国医院协会信息管理专业委员会
北京市卫生计生委信息中心
主 审 王才有 薛万国
主 编 琚文胜
副主编 刘海一 王 韬

电子工业出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书根据当前医院信息技术、医院管理和技术能力等情况,提出一种实现“可靠电子签名”的方法,解决当前数字签名技术在医院应用实施的“最后一公里”问题,实现对电子病历的“可靠的电子签名”。本书共七章,主要包括:概述,构成数字签名系统的主要内容,数字签名系统的构建与应用集成,电子病历数字签名数据结构,数字签名数据存储与访问,数字证书服务,电子病历数字签名系统建设实施过程。

本书可作为医院电子病历建设方、数字签名技术提供商和电子病历厂商提供系统建设与运行操作的指南,也可供相关领域的人员参考。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。版权所有,侵权必究。

图书在版编目(CIP)数据

医院电子病历数字签名实施指南 / 中国医院协会信息管理专业委员会,北京市卫生计生委信息中心编著; 琚文胜主编. —北京: 电子工业出版社, 2018.6

ISBN 978-7-121-34499-2

I. ①医… II. ①中… ②北… ③琚… III. ①电子签名技术—应用—病案—指南 IV. ①R197.323.1-62

中国版本图书馆 CIP 数据核字(2018)第 129259 号

策划编辑: 王晓庆

责任编辑: 王晓庆

印 刷:

装 订:

出版发行: 电子工业出版社

北京市海淀区万寿路 173 信箱 邮编: 100036

开 本: 880×1230 1/32 印张: 3 字数: 62 千字

版 次: 2018 年 6 月第 1 版

印 次: 2018 年 6 月第 1 次印刷

定 价: 36.00 元

凡所购买电子工业出版社图书有缺损问题, 请向购买书店调换。若书店售缺, 请与本社发行部联系, 联系及邮购电话: (010)88254888, 88258888。

质量投诉请发邮件至 zlts@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式: (010)88254113, wangxq@phei.com.cn。

前 言

随着医疗信息化应用的普及和深入，医院逐步使用电子病历替代传统病历，实现医疗活动过程中病历信息的记录、交换、分析和利用。电子病历能够更清晰地记录病历信息，更快速地交换和更有效地分析利用数据，在提高医疗工作效率、促进医疗协调、合理控制医疗费用和减少可预防的医疗差错等方面发挥重要作用。

然而，根据我国现行的法律体系和标准规范要求，在发挥电子病历上述系统功能时，医疗机构使用电子病历时还应采取必要的技术手段，确定电子病历数据签署人的有效认证、确保电子病历内容的完整性和可靠性，使得电子病历符合法律和法规规定的原件形式要求，以作为实现与纸质病历同等效力的举证证据。

2005年4月1日起施行的《中华人民共和国电子签名法》，在政策层面规定了电子签名同盖章和手写签名具有同等的法律效力。2017年2月，国家卫生计生委和国家中医药管理局共同印发的《电子病历应用管理规范(试行)》，再次强调医疗机构应用电子病历应当具备电子病历的安全管理体系和安全保障机制，对电子病历创建、修改、归档等操作具有追溯能力。

在技术层面，数字签名技术已经在电子商务、电子政务和金融领域的电子文档签名和认证工作中得到了广泛采用，实现了互联网环境下数据安全交换并确保数据

完整性、不可抵赖性和身份验证的法律要求。

但是由于医院数字签名场景复杂，签名对象内容各异，实现医院电子病历“可靠的电子签名”，除满足一般意义上的数字签名技术保障外，还需要根据电子病历的特点，考虑实现签名的成本、签名效能代价、签名复杂性可接受等因素，为此要合理选择签名方法和界定签名环节，采用适宜的技术手段，实现电子病历信息内容的可靠性、完整性和不可篡改性等方面的要求。

为了规范和指导我国医院电子病历数字签名系统的建设工作，中国医院协会信息管理专业委员会（CHIMA）专门立项作为研究课题，并与北京市卫生计生委信息中心、北京数字认证股份有限公司，以及医院电子病历应用和法律专家，共同撰写了《医院电子病历数字签名实施指南》，参与编写的人员有：据文胜、刘海一、王韬、王才有、薛万国、尚邦治、刘宇、陈伟、张世红、朱丽艳、樊荣、魏亮瑜、王方非、王力华、谭绍峰、曹建、赵韡、唐建立、薛雄、张秀明（排名不分先后）。

本书的编写目的是，为医院电子病历建设方、数字签名技术提供商和电子病历厂商提供系统建设与运行操作的指南，解决当前数字签名技术在医院应用实施的“最后一公里”问题，实现对电子病历的“可靠的电子签名”。

本书共七章：第一章概述，介绍医院电子病历数字签名的实现内容；第二章构成数字签名系统的主要内容，介绍电子病历数字签名系统的功能要素和组成；第三章数字签名系统的构建与应用集成，介绍医院信息系统如何与数字签名系统实现应用集成，实现数字签名功能；

第四章电子病历数字签名数据结构，介绍数字签名系统和医院信息系统实现数字签名功能所需要的数据内容和结构要求；第五章数字签名数据存储与访问，介绍数字签名数据的存储与访问控制的实现；第六章数字证书服务，介绍数字证书的服务内容和模式；第七章电子病历数字签名系统建设实施过程，介绍医院实施电子病历数字签名系统需要开展的系统运行规划、制度和 workflows 设计、医务人员培训等内容。

本书根据当前医院信息技术、医院管理和技术能力等情况，提出一种实现“可靠电子签名”的方法，实施者可根据本单位对技术复杂性、经济可接受程度和管理效率影响的接受程度，进行具体的调整和改进。

再次对本书编写工作付出贡献的专家和学者表示感谢。

王才有

中国医院协会信息管理专业委员会

CHIMA 负责人

目 录

1	概述	1
1.1	指南的目的	1
1.2	电子病历与可靠电子签名	1
1.3	电子病历的用途与数字签名需求	3
1.4	实现数字签名的原理与方法	4
1.5	数字签名系统建设的内容要点	6
1.6	数字签名的应用与管理	8
1.6.1	数字签名系统建设规划	8
1.6.2	签名的电子病历内容选择	9
1.6.3	建立数字签名系统需考虑的几项技术内容	10
1.6.4	数字签名系统应用的管理要求	12
1.7	数字签名的法律效力	14
2	构成数字签名系统的主要内容	16
2.1	数字证书	16
2.2	证书管理系统	18
2.3	数字签名验证系统	18
2.4	电子签章系统	20
2.5	时间戳系统	20
3	数字签名系统的构建与应用集成	22
3.1	应用集成架构	23
3.2	应用集成过程	24

3.3	应用集成场景	26
3.3.1	应用集成场景描述	26
3.3.2	医务人员身份认证环节	29
3.3.3	电子病历生成环节	31
3.3.4	电子病历归档环节	35
3.3.5	电子病历复制环节	36
3.3.6	电子病历封存环节	38
3.3.7	电子病历共享环节	40
4	电子病历数字签名数据结构	43
4.1	带数字签名电子病历的构成	43
4.2	电子病历内容要求	44
4.3	数字签名数据要求	44
4.4	数字签名示例	45
5	数字签名数据存储与访问	49
5.1	数字签名数据的存储	49
5.1.1	运行中的电子病历及其数字签名存储	49
5.1.2	归档后的电子病历及其数字签名存储	50
5.2	存储数据的访问	50
6	数字证书服务	51
6.1	数字证书服务内容	51
6.2	数字证书服务模式	52
7	电子病历数字签名系统建设实施过程	54
7.1	电子病历数字签名的实施条件	54
7.2	电子病历数字签名的实施步骤	54
7.3	实施数字签名的培训内容	57

7.4	数字证书发放的部门、人员	58
7.5	需进行数字签名的病历文书	58
7.6	数字签名实施的注意事项	59
附录 A	数字签名诊疗数据要素（资料性附录）	60
附录 B	数字签名应用集成实例（资料性附录）	69
附录 C	数字签名司法鉴定参考流程（资料性附录）	74
附录 D	医院数字证书使用及管理办法示例（资料性附录）	76
附录 E	医院数字证书及其介质管理细则示例（资料性附录）	79
附录 F	名词解释（资料性附录）	83
参考文献	85

1

概 述

1.1 指南的目的

应用数字签名是在电子病历中实现可靠电子签名的一种方法，也是目前电子签名法确认的各种可靠电子签名方法中比较易于实现、性价比非常高的方法。本书的主要目的是为在电子病历中实施电子签名提供指南，帮助医院实现电子病历中的可靠电子签名，同时给电子病历系统建设厂商提供引导，使其能够建设更加符合电子签名法与电子病历应用管理规范的系统。

本指南的读者是医院的信息化建设技术人员、管理人员，电子病历系统开发商的设计、支持服务人员，以及电子认证服务机构的技术人员、服务人员等。

1.2 电子病历与可靠电子签名

电子病历是指医务人员在医疗活动过程中，使用信息系统生成的文字、符号、图表、图形、数字、影像等

数字化信息，并能实现存储、管理、传输和重现的医疗记录，是病历的一种记录形式，包括门（急）诊病历和住院病历。在这些记录中的医嘱、各种检查报告、检验结果、治疗记录、病程记录、各种检查与治疗执行记录等都是重要的医疗文件。而这些电子化医疗记录中非常重要的一项内容就是医师、护士等责任人的签名确认。按照《电子病历应用管理规范（试行）》，医疗机构电子病历系统可以使用电子签名进行身份认证，可靠的电子签名与手写签名或盖章具有同等的法律效力。“可靠的电子签名”是指符合《中华人民共和国电子签名法》第十三条有关条件的电子签名。

《中华人民共和国电子签名法》（以下简称《电子签名法》）于 2005 年 4 月 1 日执行，是一项规范电子签名行为、确立电子签名的法律效力、维护有关各方合法权益的法律。电子签名法中确定了可靠电子签名的四项条件：

（1）电子签名制作数据用于电子签名时，属于电子签名人专有；

（2）签署时电子签名制作数据仅由电子签名人控制；

（3）签署后对电子签名的任何改动能够被发现；

（4）签署后对数据电文内容和形式的任何改动能够被发现。

按照《电子签名法》确定的这四项条件产生的可靠电子签名，可以保证所签署的电子文件无法被他人伪造（文件被伪造或修改时能够被发现），同时签署者也不能否认所签署的内容。

对于电子签名的概念，目前许多人存在误解，例如，一些人将手写签名的扫描图片粘贴到文件中认为是电子签名。实际上这种粘贴的签名图片与文件内容本身没有任何关联，任何人都可以在任何文件上粘贴这种图片，在法律上无法确认文件是粘贴的签名人所书写的，签名人也可以否认所书写的内容。这种仅仅在文件上粘贴图片的方法不是可靠的电子签名，因而带有签名图片的电子文件无法作为法律上的证据使用。

数字签名是一种应用数学加密的方法来产生与文件内容关联的签名，加密的签名数据通过数学证明在现有条件下无法破解或伪造，同时这种签名又可以被特定的机构进行验证。利用数字证书技术产生的数字签名能够满足《电子签名法》所要求的四项基本条件，是一种被法律认可的“**可靠电子签名**”。按照目前的电子技术水平、管理条件，应用数字签名技术作为实现电子病历中可靠电子签名的方法在经济上、技术上和管理上都具备可行性。

1.3 电子病历的用途与数字签名需求

作为医疗过程中产生的记录，电子病历有多种用途，包括：用于医疗过程中作为医院各项检查、治疗环节进行信息沟通交换的媒介；患者在不同医疗机构之间就医时的信息传递文件；出现医疗纠纷时举证的证据；医疗经验总结的依据；医疗教学的案例；医学研究的基础数据来源等。在这些不同的用途中，对于医疗记录责任确

认的要求强度大不相同。其中，对“出现医疗纠纷时举证的证据”的责任确认要求最高，通常要求能够经过第三方认证。对于“用于医疗过程中作为医院各项检查、治疗环节进行信息沟通交换的媒介”、“患者在不同医疗机构之间就医时的信息传递文件”的责任确认要求相对弱些，通常在医疗机构内部采用信息系统认证，在医疗机构之间采用机构认证签名即可。对于教学、科研等应用，则通常不需要责任确认。

对于病历记录的签名要求，《病历书写基本规范》中给出了明确要求。这个规范中规定了门诊病历、住院病历的内容，并在第八条中要求“病历应当按照规定的内容书写，并由相应医务人员签名”。电子病历是采用电子方式实现《病历书写基本规范》要求内容的记录，同时，由于电子病历能够包含图形、图像、视频等多种媒体，因此其内容有时比纸张病历更多。数字签名是一种符合《电子签名法》要求的可靠电子签名，电子病历中使用数字签名在多数情况下能够实现手工签名的功能，从而可以替代手工签名。

1.4 实现数字签名的原理与方法

数字签名的基本原理是利用非对称加密技术对电子文件进行加密运算产生签名，用签名数据还原的文件（或摘要）与原文（或摘要）进行比对来确认原文是否被修改。非对称加密技术是一种数学方法，这种方法对文件的加密和解密使用不同的密钥。签名时使用的**加密密钥**

是私钥，仅由签名人掌握；验证文件时使用的**解密密钥**是公钥，可以在公开场合传输。数学方法保证无法通过解密公钥推算出加密私钥的内容。

在实际应用中，签名人往往需要使用一个存储介质（如 U-KEY、IC 卡或手机等）来进行数字签名的操作，这个存储介质中存放着数字证书，其作用是证明签名人的身份。这个数字证书是由权威的认证机构产生与管理的一种数字文件，在这个文件中包含公开密钥、拥有者、签发者、有效期及一些扩展信息。在需要时利用数字证书中存储的信息到认证机构进行查证，即可确认签名人的身份信息及签名的有效性。

通常用于签名的加密私钥也存储在签名人掌握的存储介质中，因而其他人无法掌握和使用签名的私钥。为防止存有私钥的介质丢失后被他人利用，在使用私钥进行签名时还需要签名人输入 PIN 码（个人识别码），来保证确实是签名人在使用私钥进行签名操作。

图 1.1 所示为数字签名过程与验证过程示意图，通常在医院电子病历各系统中使用的是数字签名的过程，通过这个过程产生的签名密文文件保存在系统中。当需要进行验证时，将原文文件、签名密文文件及签名人的数字证书一同提交，由权威机构或经过认证的验证系统进行验证处理，通过比对验证中产生的两个摘要信息的一致性，来判断原文是否被篡改。

我国的法规对于医务人员有比较完善的管理体系，医院也有相应完善的制度，因此应用数字签名技术解决电子病历中医务人员的责任识别与认定具有较好的可

操作性。而在目前病历中的患者知情同意书等需要患者签名的文件中，由于患者的唯一识别没有统一的管理机制与手段，因此需要更加复杂的设备与方法来解决患者签名的问题。本书后面的各章中会对相关问题给出解决方案。

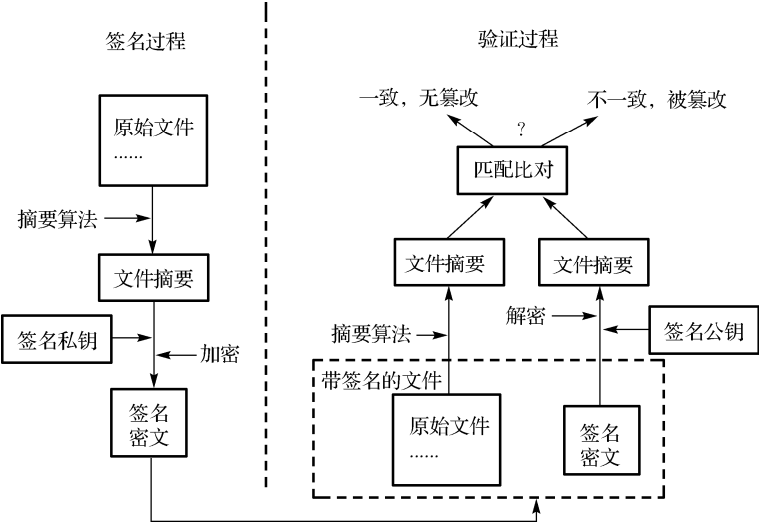


图 1.1 数字签名过程与验证过程示意图

1.5 数字签名系统建设的内容要点

目前许多医院已经建立起一系列电子病历信息处理的信息系统。但如果医院需要在电子病历中实现电子签名，则还需要建立一套支持电子签名的基础环境，以支持电子病历中各系统进行可靠电子签名。这个环境包括：从经过认证的机构获得数字证书的管理系统、每个医务人员存储证书的介质、将数字签名处理工具嵌入到电子

病历各专业系统、签名管理与存储系统、签名展示工具、数字签名认证工具等。

为保证医务人员能够在日常工作中高效地完成签名操作，通常需要数字证书的发证机构与电子病历的各系统开发商密切配合，将数字签名的操作完全融合到日常的信息系统使用过程中，使医务人员感到使用数字签名比手工签名还要方便。

医疗记录中的时间是非常重要的信息。纸张病历中对于各种时间的记录就有比较严格的要求，因此在电子病历的记录中同样应实现对时间内容的完整、可靠记录。通常在医院建立电子病历体系时或在建立数字签名体系时，应同步建设好时间同步系统。按照《电子病历应用管理规范（试行）》的要求，电子病历系统记录的时间应该来源于不受医院控制的可靠时间源，以保证电子病历记录中时间的公正、可靠。在数字签名系统中同时加入时间戳的方法是一种比较便捷、可靠的时间记录方式。这时，数字签名记录就应该选择带有时间戳的签名记录格式，以保证时间戳能够正确地记录签名时间并保存在签名的数据中。

为使医院电子病历系统所产生的可靠电子签名得到认可，医院的数字签名系统建设应该符合国家制定的相关标准。我国的《电子签名法》是确认电子签名法律效力的基本文件，系统的建设应该符合《电子签名法》中有关可靠电子签名中的基本要求。《电子病历应用管理规范（试行）》（国卫办医发〔2017〕8号）是卫生行业对于电子病历、电子病历中电子签名的行业要求与规范，

这个规范细化了《电子签名法》中的实施要求，使得电子病历与电子签名能够在实际工作中施行。《卫生系统电子认证服务管理办法（试行）》（卫办发〔2009〕125号）规定了卫生系统可以按照《电子认证服务管理办法》（工业和信息化部令 2009 年第 1 号）的要求选择电子认证服务机构实施电子认证相关的处理，使数字签名能够落地实现。在具体技术实现时，电子病历系统开发商与电子认证服务机构可以按照《信息安全技术 公钥基础设施 电子签名格式规范》（GB/T 25064—2010）的要求，选择带有时间戳的电子签名格式作为电子病历中数字签名的记录标准。

1.6 数字签名的应用与管理

1.6.1 数字签名系统建设规划

在电子病历体系中建立的数字签名系统是电子病历体系中非常重要的组成部分，数字签名记录关系到电子病历记录的有效性。对于医院的数字签名系统建设，有多个方面应该认真考虑，包括：签名有效性保证、签名针对的文件内容、系统建设与运行的投资、病历记录长期存储的容量、可读性与可验证性、签名过程应用的方便性、数字证书介质的可管理等。这些需要考虑的问题远超出技术的范畴，需要医院从管理、经济、技术、法律等多方面综合权衡。因此在建设数字签名系统之前，从全院整体角度做好规划是一项重要的工作。在这个规

划中，首先应该明确建设电子病历体系和数字签名系统要解决的主要问题或目标，如数字签名主要用于应对电子病历记录的法律认可问题、实现绝大部分病历的无纸化记录与传输、建立全面无纸化病历体系等。不同的目标在整个电子病历体系建设的投资、管理方面有巨大的差别。同时在规划中应该针对设定的目标对所需要建设的系统规模、投资、应用流程、管理要求等进行评估，使决策时心中有数。

1.6.2 签名的电子病历内容选择

电子病历内容繁多，其内容往往比现有纸张病历的内容多出许多，对全部内容都用数字签名的方式进行责任确认需要比较大的投资。对于一些只在医院内部传输、用于医疗过程交换的记录，进行完整的电子签名也不一定有很大的必要。例如，对于那些在医院做无过错举证时使用不到的内部过程信息记录，全部都要求进行可靠电子签名，其实际作用也不大。因此，医院对于哪些内容需要进行数字签名处理，应该从实际需要出发，进行仔细选择。

医院中常用的需要签名的电子病历的内容包括：病历记录、医生下达的医嘱、处方、各种检查报告、检验报告、手术记录与麻醉记录、重症监护记录、诊断证明等。这些需要签名的内容的共同特点是它们都是医疗中的结果记录。而对于那些医疗过程产生的中间记录，则在对外举证时很少使用，如检查申请、检验申请、药房配药记录等。

在实际应用时，医院往往还需要为患者、管理部门、法律机构等医院之外的个人或机构提供病历文件，在这些文件中除需要有医疗执行人员个人的签名外，医院还需要对整份文件再进行签章确认。在这种情况下，不仅对具体病历文件内容需要有医务人员的个人数字签名，医院还需要将提供给患者、管理部门或法律机构的电子病历内容打包整理，并再次用医院的数字证书进行数字签名处理，相当于在提交的病历上盖上医院图章。

1.6.3 建立数字签名系统需考虑的几项技术内容

在数字签名系统的建设中，根据实现应用功能的需要，一些技术实现上的功能是在建设中应该考虑的内容。除一些数字签名必备的功能外，一些特殊的应用功能也对电子病历应用有很大的影响。

1. 签名中的时间戳

医疗记录的产生时间对于举证有非常重要的作用，因此电子病历中的数字签名包含时间戳是医疗文件签名的一项重要要求。医务人员使用个人控制的私钥对所书写的医嘱、病历、检查报告、检验记录、治疗记录等进行签名，解决了这些医疗记录的责任认定问题。但是基本的数字签名并没有包含签名的时间。一个完整的签名还应该在对内容进行基本签名后及时对产生这些签名的时间再进行可信的认证，即用一个时间戳来可信地记录这些签名产生的时间。这个时间戳的产生需要三个基本内容：首先是需要包含医务人员的签名，其次是不受医院控制的标准时间源，第三是对医务人员签名与时间

的可靠的数字签名。按照这样的需求，电子病历系统中数字签名记录的格式应该使用《信息安全技术 公钥基础设施 电子签名格式规范》（GB/T 25064—2010）中的 ES-T 或更完整的签名格式。

2. 标准时间源

为了能够在电子病历记录中产生有效的时间戳记录，系统中的时钟同步体系和守时系统有非常大的影响。维持信息系统中时钟的准确及同步，需要让系统中各台计算机与标准时间源保持同步。常用的标准时间源包括：通过互联网连接国家授时网站获得的标准时间，通过 CDMA 手机信号获得的标准时间，使用北斗或 GPS 导航卫星获得的标准时间，利用国家长波授时台广播信号进行时间同步获得的标准时间等。由于医院信息系统的连续运行能力与整个医院业务的运行密切相关，因此系统中需要有一定的容错功能，即当外部的时钟源出现问题时，系统仍然能够正常运行，数字签名不因时间源短时的中断而影响整个电子病历记录的生成。这种情况下应该在时间戳体系中配备一个由第三方控制的守时系统，当外部的时间源信号中断后，在一段时间内能够使用于签名时间戳的时间系统保持一定的精度。根据医疗法规要求，手工的医疗记录通常只需要精确到分钟。在电子病历中，这个记录的时间如果能够保持在 1 秒以内，就能够满足要求。在现在的技术条件下，医院的守时系统能够在比较长的时间内（如 1 周、1 个月等）让时间系统保持在高于 1 秒的精度范围内，这样能够使医院的电子病历系统的运行较少受到外部标准时钟体系故障或网络故障的影响。

3. 签名的日志记录

医院的电子病历体系中各个专业的医疗信息处理系统随时都会产生电子签名记录。在应用这些病历记录与签名记录进行举证时，保持电子病历记录的不缺失也是一项重要的应用需求。因此在电子病历的数字签名系统建设时，需要一种方法能够记录每一项签名，一旦出现签名记录缺失就能够发现。这种签名的日志记录系统应该在医院的数字签名系统设计和建设时就进行规划。实现这种签名的日志记录可以通过数字证书提供商（电子认证服务机构）的系统在签名时产生日志，也可以在数字签名的应用系统中生成签名日志。一种比较简便的方法是医院中所有数字签名都通过一个统一的签名服务程序实现，这个签名服务程序包含签名的日志记录功能。在这个功能中可以定时（或签名达到一定数量时）对已经完成的签名日志进行签名，以保持日志不被篡改。

1.6.4 数字签名系统应用的管理要求

实现数字签名应用不仅需要系统建设和技术保障，还需要有配套的管理体系对数字证书发放、签名操作流程、需签名电子病历内容选择、病历记录与签名记录的存储、病历提供或举证文件提供时的再签名规范等内容进行管理。这些管理的内容不仅与电子病历本身有关，还与医疗流程和业务相关的管理制度密切相关。

对于数字证书的发放管理，医院应该制定完善的证书发放、使用、补发等制度。这些制度应该与医生、护士、技术人员的职业资格管理制度相关联。在一些制度

比较完善的医院中，数字证书的使用还应该与医务人员的职务行使权相连接。为了保证医疗工作的连续性，需要充分考虑制度中一些特殊的内容。例如，一人多个证书的管理、忘记带证书介质时临时签名证书的管理及签名记录的处理、教学医院实习生证书与签名方式的管理等。

在签名操作流程上，需要充分考虑平衡签名的可靠性与日常医疗操作的方便性。通常为防止介质丢失后被其他人冒用而失去签名的唯一性，数字证书使用时需要使用人输入 PIN 码进行确认。但如果每次签名都需要输入 PIN 码，则会大大影响工作效率。一个比较平衡的操作流程，可以在系统中设置第一次使用数字证书时要求输入 PIN 码，如果在一定时间间隔内连续进行签名，则不必再输入 PIN 码。当系统闲置一定时间后，可以要求再次输入 PIN 码进行认证。

电子病历文件的再签名处理是医院向外部提供病历时的常用功能。医院应该针对这些病历提供的内容、流程、签名方法做出相关的管理规定。医院可以在电子病历书写完成后设定归档状态。根据不同的需要，医院可设定电子病历不同的归档内容，例如，针对患者复制病历的归档，针对卫生管理部门的管理病历归档，针对完整病历记录的全病历归档，针对医务人员医疗、教学、科研使用病历的归档等。对于各类归档的病历，医院可以在归档时应用医院的数字证书对其进行签名。经过签名的电子病历可以随时提供给需要的使用者。

1.7 数字签名的法律效力

在涉及医疗的法律诉讼中，通常需要由医院提供各种证据，病历是最常用的一种证据。当病历作为法律证据时，其真实性是最重要的属性。需要确认的真实性主要包括病历是否由医疗机构产生、是否由当事医务人员记录、病历的书写时间。在使用纸张病历时，这些属性通常通过病历书写人的签名认定。当对真实性有疑问时，可以通过笔迹鉴定给出第三方的证明。当使用电子病历作为证据时，同样需要确认其真实性。依据《电子签名法》，病历的书写者使用符合“可靠电子签名”的方式进行签名后，病历的真实性就可以通过第三方对病历及签名的鉴定进行确认。符合规范的数字签名是一种可靠电子签名，因此可以起到纸张病历中与手工签名同样的作用。经过数字签名的病历，别人是无法伪造的，对病历内容进行的任何修改都可以被发现，同时签名中所包含的时间戳也记录了不受医疗机构和病历书写者控制的签名时间。在需要确认病历的书写者、书写时间时，提供数字证书的机构就有义务且有手段依据签名对病历的真实性提供鉴定，确认病历内容是否由书写者书写、病历内容是否在签名后被修改过，以及书写病历的时间。当电子病历的这些属性被确认后，其作为真实的医疗记录，在法律诉讼中就能够满足作为证据的条件。

与手工签名的纸张病历相比，带有电子签名的电子病历对于书写时间的记录更加准确，鉴定和确认也更加

容易。根据医疗法规和管理制度，在医疗过程中病历是允许修改的，但修改过的病历需要保留痕迹。应用纸张病历时，这些修改需采用各种保留痕迹的方式记录在原病历中。而对于电子病历，经过签名后病历如果修改，就需要用记录不同版本并再签名的方式保留修改的痕迹。使用数字签名对修改的病历再次签名时，签名数据中的时间戳记录了再次修改的时间。这种方式比纸张病历的记录更能反映实际发生的情况。

为使数字签名的应用能够更好地保证电子病历的法律效力，数字签名系统应该严格按照相关要求建设与管理。特别是系统设计、设备选择与配置、证书的发放与管理都应该满足可靠电子签名所需要的各种保障条件。后续的各章节将详细介绍相关的建设与管理的技术细节。

2

构成数字签名系统的主要内容

在医院中，构成电子病历的数字签名系统主要包括：证书管理系统、数字签名验证系统、电子签章系统、时间戳系统等。这些系统通常都是由经过国家认证授权的第三方电子认证服务机构或相关软件开发机构提供的。医院将数字签名系统中的有关功能与医院各类信息系统进行应用集成，就可以实现基于数字证书的电子病历数字签名。通过在电子病历中应用带有时间戳的数字签名，实现医疗数据的完整性保护、可信时间记录、责任认定等需求。下面给出构成数字签名系统的详细说明。

2.1 数字证书

数字证书（非对称密码体系中的“公钥”）是网络中证明机构或个人身份有效的数据文件。它是由权威机构——第三方电子认证服务机构颁发的，用于在网上对机构或个人身份进行标识的文件。数字证书相当于认证机构盖

在数字身份证上的一个章或印（类似于实体身份证上公安局盖的章）。

数字证书包括持有者信息、有效期、颁发机构信息、颁发机构对证书基本信息的数字签名及签名算法等内容。对电子病历进行数字签名时，使用的是数字证书持有者对应的“私钥”。数字证书及其持有者“私钥”通常以某种介质作为载体。用于存储个人签名的数字证书介质一般有 USB Key、蓝牙 Key、IC 卡、手机等；用于机构或系统签名的数字证书，其介质除可使用上述载体外，有时也会将其存储在密码服务器中。

用于电子病历数字签名的数字证书至少应满足如下要求：

（1）第三方电子认证服务机构应符合《卫生部电子认证服务管理办法（试行）》的相关要求；

（2）数字证书算法应采用 SM2 密码算法；

（3）数字证书格式应符合《卫生系统数字证书格式规范（试行）》的相关要求；

（4）数字证书载体应具备数字证书及私钥的存储安全保障机制，应具备数字证书持有者的身份校验机制，并满足医务人员在移动医疗、PC 端诊疗等场景中执行电子病历数字签名的功能要求；

（5）持有人为个人时，签名人应妥善保管数字证书及其私钥，并负责确保数字证书载体用于校验身份的信息由本人控制，数字证书不得转借他人使用。

2.2 证书管理系统

证书管理系统是实现医务人员数字证书全生命周期管理服务的工具。医院中的电子病历系统若要能够实现数字签名，每个数字证书必须能够与持有人（如使用数字证书进行签名的医务人员）进行关联，并有完整的记录。每个数字证书只能关联一个需要签名的医务人员。通过使用证书管理系统，医院的管理者就能够方便地完成证书的签发、自动更新、吊销等证书相关业务处理，保证数字证书使用的方便性、连续性。

证书管理系统至少应满足如下要求：

（1）提供数字证书的全生命周期管理的各种处理功能，至少包括证书申请、证书审核、证书下发、证书更新、证书废止功能；

（2）应满足医院内网封闭环境下医务人员数字证书的自动更新需求。

2.3 数字签名验证系统

数字签名验证系统是实现基于数字证书的实体用户（如医务人员、患者、设备、系统等）身份识别、电子病历数字签名及签名验证服务的密码产品。通俗来讲，纸质文件签名是为了表示这份文件是签名者所写。同理，数字签名的意义在于证明文件是某个特定的人编写的（文件的有效性）、证明文件没有被篡改（文

件的完整性)。当数字证书实体用户使用数字证书访问业务系统进行登录、数字签名时,数字签名验证系统用于实现身份认证、数字签名及验证,保证消息的有效性、完整性。

签名验证系统至少应满足如下要求:

(1) 应采用 **SM2**、**SM3** 密码算法;

(2) 应符合国家密码管理局关于密码产品的相关要求,且符合《卫生系统数字证书应用集成规范(试行)》等标准的相关要求;

(3) 应提供基于数字证书的身份识别功能,支持不同第三方电子认证服务机构的证书验证,提供 **CRL/OCSP** 等多种方式的证书有效性验证;

(4) 针对患者手写数字签名功能应提供签名人数字证书签发服务,证书内容应包括签名人的身份特征信息,如手写签名笔迹、照片、指纹等;

(5) 应提供基于签名人数字证书的数字签名及签名验证服务,保证电子病历内容的完整性、有效性和签名行为的不可否认性;

(6) 针对患者手写数字签名功能应能够确保签名人数字签名仅对当次有效,即每次执行电子病历数字签名前,应重新鉴别签名人身份特征信息;

(7) 能够存储数字签名日志,存储内容包括数字签名流水号、原文的唯一序列号、患者唯一标识、患者姓名、签名人姓名、电子病历原文 **Hash** 值、数字签名值、时间戳值、签名人数字证书等信息,并可实现对每条数字签名日志的数字签名。

2.4 电子签章系统

电子签章系统用于实现电子病历中数字签名的可视化展现，使数字签名能被人们看到。电子病历的各个系统通过调用电子签章的处理程序，完成电子病历签名状态的显示功能。

在实际应用中通常利用图像处理技术将数字签名操作转化为与纸质文件签字或盖章操作类似的可视效果。但电子签章不同于单纯的签字图片与文件的剪贴，电子签章进行的处理由数字签名技术作为支撑，通过处理程序来实现数字签名与病历内容的关联展现。人们使用这个工具来掌握文件是否经过数字签名。

电子签章系统至少应满足如下要求：

（1）应与数字签名验证系统一致，符合国家密码管理局关于密码产品的相关要求，且符合《卫生系统数字证书应用集成规范（试行）》等标准的相关要求；

（2）应提供签名人电子签章存储的安全保障机制，实现电子签章与数字证书的有效绑定，电子签章能够用于数字签名的展现与验证；

（3）应提供签名人电子签章的验证功能，对于展现的经数字签名的电子病历，能够验证签名人电子签章的有效性并呈现验证结果。

2.5 时间戳系统

电子病历作为医疗记录，按照法规的要求必须有责

任人签名和准确的时间记录，因此电子病历如使用数字签名，也必须是带有时间戳的数字签名。时间戳系统就是用于在电子病历中加盖时间戳，确保时间准确、可信的工具。为保证电子病历中的时间戳能够具备法律上的可信度，它的时间必须源自权威、可靠的时间源，并具备权威第三方电子认证服务机构的数字签名。

时间戳系统所使用的时间源应来自于权威的授时体系并有一定的精度，以保证时间的准确、可靠。同时考虑医院应用不能中断，时间戳系统中还必须拥有较高精度的守时功能，以保证在网络或外部时间源发生中断时，医院仍然能够在一定时间内执行时间戳的生成及数字签名处理。

时间戳系统至少应满足如下要求：

（1）应与数字签名验证系统一致，符合国家密码管理局关于密码产品的相关要求，且符合《卫生系统数字证书应用集成规范（试行）》等标准的相关要求；

（2）应提供签发时间戳、验证时间戳有效性的功能；

（3）时间戳应基于不受医院控制的权威、可靠的时间源，以确保时间的准确和可信，时间源通常来源于北斗 2、GPS、CDMA 等多种方式；

（4）应提供时间同步功能，基于国际标准 NTP 或 SNTP 协议，从时间源获取时间并同步，时间同步精度到毫秒。

3

数字签名系统的构建与应用集成

为能够在医院中方便地对电子病历系统中实施数字签名，需要将数字签名系统与电子病历系统进行集成。在上一章中已经列出了数字签名系统的四个主要系统，其中最主要的数字签名验证系统、电子签章系统及时间戳系统需要与医院的电子病历系统进行集成。

数字签名验证系统、电子签章系统、时间戳系统通常需要与电子病历系统中的各个专门处理功能进行比较深度的集成，通常需要将数字签名相关功能嵌入到电子病历的应用系统中，常用集成包括以下几个环节。

（1）在电子病历系统中需要进行签名的地方嵌入数字签名处理模块，例如，在完成病历书写后进行提交时、医嘱下达后进行确认时等。这个环节的集成是实现数字签名的基本功能，所有实现数字签名的电子病历系统都不应该缺少这个环节。

（2）在电子病历显示或打印时需要嵌入电子签章处理模块进行签名的展现，例如，病程记录的显示、打印，

医嘱的显示与打印功能。这个环节的集成用于实现数字签名可视化展现功能。

（3）在病历归档、向患者或外部机构提供病历数据时需要嵌入数字签名处理模块，此时通常使用医院的数字证书对提供给患者或外部机构的病历数据进行签名，以确认所提供的数据是经过医院认可的。此类环节通常包括病历复印、病历封存、病历归档处理等。嵌入签名的方式与病历提交时的签名类似。

下面给出数字签名系统与电子病历系统进行集成相关的详细说明。

3.1 应用集成架构

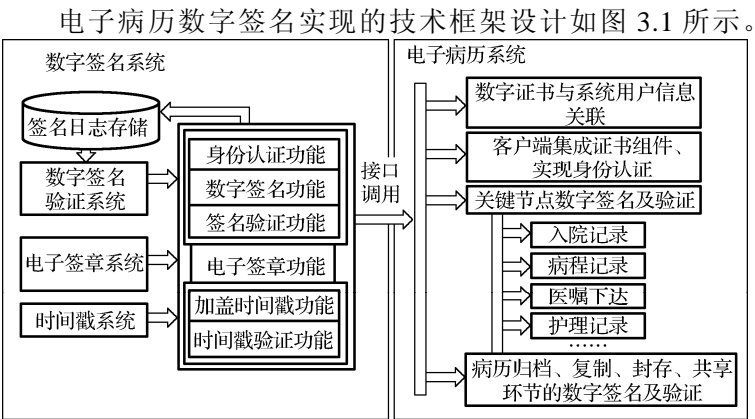


图 3.1 电子病历数字签名实现技术框架图

医院信息系统包括 HIS、EMR、LIS、PACS 等多类临床信息处理系统，是电子病历的生产系统，以产生、流转、存储电子病历等业务为主。由于各类医院信息系

统在实现电子病历各业务环节数字签名应用方面具有通用性，因此本书仅说明电子病历各业务环节数字签名应用的实现方案，并以泛指电子病历系统为例，各类医院信息系统均可参照实现。

电子病历系统需要与数字签名系统中各功能组件集成，以接口调用的方式实现用户基于数字证书的身份认证、重要业务环节的数字签名及签名验证、电子签章、时间戳加盖及验证。此外医生工作站、护士工作站 PC 端也需要部署数字签名应用环境并与电子病历系统客户端集成，以配合电子病历系统服务端，实现数字签名应用。

3.2 应用集成过程

对于医院来说，各类医院信息系统的开发模式有两种：C/S 和 B/S。C/S 又称 Client/Server 或客户/服务器模式。服务器通常采用高性能的 PC、工作站或小型机，并采用大型数据库系统，如 Oracle、Sybase、Informix 或 SQL Server。客户端需要安装专用的客户端软件。B/S 是 Browser/Server 的缩写，客户机上只需要安装一个浏览器（Browser），如 Netscape Navigator 或 Internet Explorer，服务器上安装 Oracle、Sybase、Informix 或 SQL Server 等数据库。浏览器通过 Web Server 与数据库进行数据交互。

根据各类医院信息系统的开发语言和开发模式的不同，第三方电子认证服务提供商给医院信息系统开发商提供对应的接口文档，共有四类：Java 版、COM 版、C 版和 Web Service 版。

以 COM 版接口为例，介绍电子病历系统数字签名应用集成过程。

(1) 电子病历系统开发商配置电子病历系统的签名验证接口及时间戳接口

在电子病历系统服务端配置签名验证接口及时间戳接口，接口形态为 COM 组件，电子病历系统客户端也需要配置签名验证接口及证书载体的应用接口，接口形态一般分为 ActiveX 控件和 DLL 动态库两类。具体签名验证接口及时间戳接口的调用方法及接口定义可参考《卫生系统数字证书应用集成规范》。

在每次执行数字签名、时间戳后，应及时进行签名及时间戳验证。

(2) 电子病历系统开发商修改电子病历系统数据库

① 在电子病历系统医务人员用户表中需要增加“数字证书唯一标识”字段，用于建立数字证书与电子病历系统医务人员账号之间的对应关系；

② 在电子病历系统数据库中保存数字签名数据，并建立数字签名数据和对应电子病历原文的关联关系。

(3) 电子病历系统开发商在电子病历系统身份认证场景下的应用集成工作

电子病历系统开发商在电子病历系统身份认证场景下的应用集成工作包括：

① 修改电子病历系统登录页面，嵌入证书控件，将普通用户名口令登录页面修改为证书登录界面；

② 修改电子病历系统登录按钮，加入证书控件的调用脚本，并由签名验证系统对电子病历系统客户端提交

的身份认证信息进行验证。

(4) 电子病历系统开发商在电子病历系统各业务场景下的数字签名应用集成工作

电子病历系统开发商在电子病历系统各业务场景下的数字签名应用集成工作包括：

① 电子病历系统需要在电子病历生成、归档、复制、封存、共享等业务场景中的电子病历提交页面中加入调用数字签名服务的脚本程序，实现对电子病历的数字签名，并将电子病历原文、数字签名值等数据打包上传至电子病历系统服务端；

② 电子病历系统服务端接收程序调用相关数字签名服务接口，由签名验证系统进行数字签名验证、时间戳系统加盖时间戳、电子签章系统加盖电子签章，并将签名数据存入数据库中保存，同时在签名验证系统中保存签名日志。

3.3 应用集成场景

3.3.1 应用集成场景描述

电子病历数字签名应用场景主要包括医务人员身份认证、电子病历生成环节、归档环节、复制环节、封存环节和共享环节。本书提供了数字签名在上述场景中的应用集成的最佳实践方法，并说明了各场景中数字签名应用的目的和意义。

各数字签名应用场景描述如下。

（1）医务人员身份认证。医务人员登录电子病历系统时以数字证书作为有效身份凭证，实现基于数字证书的高安全性、高可靠性的登录认证，能够保证医务人员在电子病历系统中的身份真实可信。根据所采用的数字证书载体的不同，医务人员在登录电子病历系统进行身份认证时校验身份的方式也会有所区别。以 USB Key 与手机两种证书载体为例，医务人员登录电子病历系统使用 USB Key 进行身份认证时，需要将 USB Key 插入计算机并输入 PIN 码；医务人员登录电子病历系统使用手机进行身份认证时，需要通过扫描登录二维码，并进行指纹识别或输入 PIN 码。

（2）电子病历生成环节。医务人员通过电子病历系统编写完成电子病历后，以及患者或患者家属对知情同意类文书进行知情确认后，医务人员、患者或患者家属分别通过执行数字签名，保证电子病历真实完整、合法可信。

对于类似各科室医生通过 EMR 系统、LIS 系统、PACS 系统等编写病历、处方、医嘱、住院记录、手麻记录、检验检查报告等文档的场景，需要责任医生在编写、修改、审核完成后执行数字签名，在执行数字签名时需要校验签名人身份，校验方式与身份认证时相同，签名后会在文档相应位置显示医生的电子签章。

对于类似护士使用移动终端设备通过移动医疗 APP 软件执行医嘱、录入护理记录等的场景，需要责任护士在编写完成后执行数字签名，在执行数字签名时需要校验签名人身份，校验方式与身份认证时相同，签名后会在相应位置显示护士的电子签章。

对于类似患者或患者家属签署由医生通过 EMR 系统编写的知情同意类文书的场景，需要在阅读后由患者执行数字签名。在执行数字签名时，需要采集患者或患者家属的手写笔迹、影像、指纹等生物特征以明确身份，再基于生物特征信息通过为患者签发事件性数字证书完成对文档的数字签名，签名后会在相应位置显示患者或患者家属的电子签章。

（3）电子病历归档环节。电子病历归档时需要通过验证归档病历中所含数字签名有效性，保障归档电子病历的真实性、完整性，再由电子病历管理部门对确认归档的电子病历执行数字签名，能够保证归档电子病历真实完整、合法可信。

（4）电子病历复制环节。电子病历复制时需要通过验证复制部分的电子病历中所含数字签名的有效性，保证复制部分电子病历的真实性、完整性，再由电子病历管理部门对电子病历执行数字签名，能够保证复制电子病历真实完整、合法可信。

（5）电子病历封存环节。确定封存电子病历的范围后，需要对电子病历进行复制并验证复制部分电子病历所含数字签名的有效性，再由医患双方或双方代理人共同对封存的电子病历进行数字签名，能够保证封存电子病历真实完整、合法可信。

（6）电子病历共享环节。在共享电子病历发送前，需要验证电子病历中所含数字签名的有效性，再由发送医院对共享电子病历执行数字签名，能够保证共享电子病历真实完整、合法可信。接收医院接收到电子病历时，

需要验证发送医院电子病历数字签名的有效性，能够保证共享电子病历真实完整、合法可信、来源真实。

3.3.2 医务人员身份认证环节

医务人员登录电子病历系统进行身份认证时，涉及医务人员、电子病历系统、数字签名服务三类角色，其角色描述如表 3.1 所示。

表 3.1 医务人员身份认证场景角色描述

角 色	事 件 描 述
医务人员	数字证书持有人，在客户端发起登录请求，输入 PIN 码进行电子病历系统登录
电子病历系统	判断登录人员权限，调用数字签名服务身份认证接口
数字签名服务	医务人员数字证书有效性验证，数字签名验证

在电子病历系统中，医务人员的身份识别采用数字证书方式的身份认证，根据数字证书载体的不同，如采用 USB Key 或手机等，其身份认证的方式有所区别，使用 USB Key 时需要医务人员将 USB Key 插入 PC 端，而使用手机则可能需要通过扫描二维码的方式，但电子病历系统的身份认证实现流程是类似的，具体实现流程如图 3.2 所示。

医务人员身份认证环节的应用集成关键点包括以下两方面。

(1) 证书注册绑定

电子病历系统开发商需要在电子病历系统医务人员用户表中增加“数字证书唯一标识”字段，用于建立数字证书与电子病历系统医务人员账号之间的对应关系。

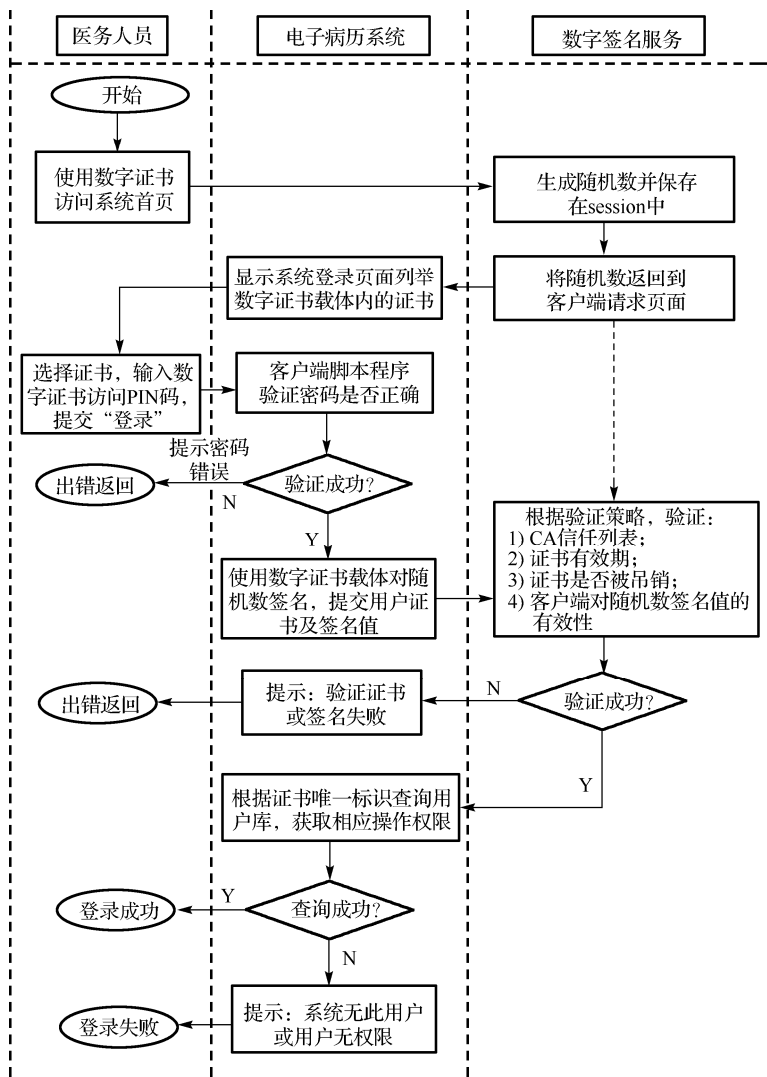


图 3.2 身份认证实现流程图

(2) 基于数字证书的身份认证

基于数字证书的登录认证过程中，电子病历系统需

要调用数字签名相关服务实现对医务人员数字证书访问口令的校验、基于随机数的签名和验证、验证医务人员数字证书的信任链、验证医务人员数字证书有效期、基于最新的黑名单文件验证医务人员数字证书是否被吊销等。

3.3.3 电子病历生成环节

当医务人员通过电子病历系统编写完成电子病历后，需要对电子病历进行数字签名，该业务环节定义为电子病历生成环节，在该环节中根据签名主体的不同，分别介绍医务人员、患者的电子病历数字签名的应用集成过程。

1. 医务人员电子病历生成环节数字签名

医务人员电子病历数字签名场景涉及医务人员、电子病历系统、数字签名服务三类角色，其角色描述如表 3.2 所示。

表 3.2 医务人员电子病历生成环节数字签名场景角色描述

角 色	事 件 描 述
医务人员	数字签名主体，在客户端发起签名请求，输入 PIN 码验证数字身份有效性，进行电子病历数字签名
电子病历系统	调用签名验证接口、时间戳加盖及验证接口
数字签名服务	医务人员数字证书有效性验证，数字签名及验证、时间戳加盖及验证、保存签名日志

电子病历文档来自不同的业务系统，如检验检查报告是在 LIS、PACS 系统中生成的，住院病历、医嘱等是在 EMR 系统中生成的，因此，当医务人员到医院各类信息系统中编写完毕电子病历后进行数字签名时，需要由生成该电子病历的信息系统在当前节点调用数字签名服

务、时间戳服务实现数字签名、时间戳，成功后会在病历的相应位置显示签名人的电子签章。

具体实现流程如图 3.3 所示。

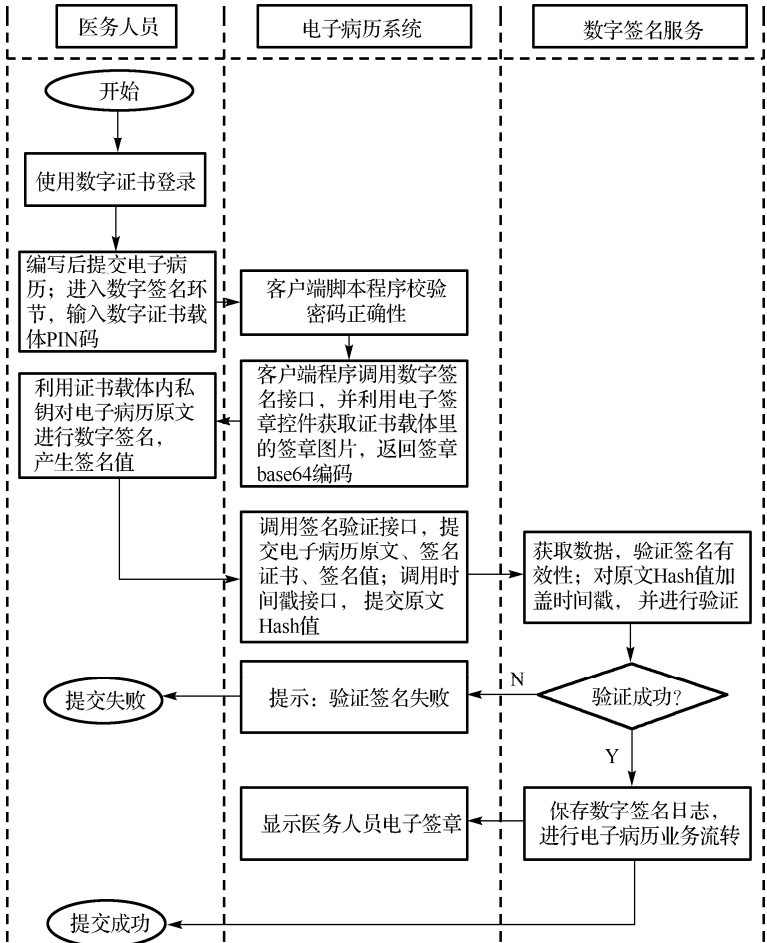


图 3.3 医务人员电子病历生成环节数字签名实现流程图

医务人员电子病历生成环节数字签名的应用集成关键点包括以下几方面。

(1) 数字证书访问 PIN 码确认

医务人员在使用数字证书的机制执行数字签名操作时，要先进行数字证书访问控制 PIN 码确认。

(2) 数字签名及验证

医务人员进行数字签名操作后应及时进行数字签名验证，同时加盖电子病历时间戳认证，并显示医务人员电子签章。

(3) 数字签名电子病历原文获取

电子病历原文需要由电子病历系统开发商根据电子病历的展示规则拼装获取。

2. 患者知情同意类文书确认数字签名

患者知情同意类文书数字签名场景涉及患者、医务人员、电子病历系统、数字签名服务四类角色，其角色描述如表 3.3 所示。

表 3.3 患者电子病历数字签名确认场景角色描述

角 色	事 件 描 述
医务人员	编辑知情同意类文书，生成知情同意类文书并对患者讲述
患者	知情同意类文书数字签名主体，通过客户端签名设备采集手写签名笔迹及其他身份特征申请事件性数字证书，完成知情同意类文书数字签名
电子病历系统	调用数字签名验证接口、时间戳加盖及验证接口
数字签名服务	为患者签发事件性数字证书，进行数字签名及验证、时间戳加盖及验证，并保存签名日志

患者对知情同意类文书进行知情确认时，由生成该知情同意类文书的信息系统在当前节点调用数字签名服务、时间戳服务实现数字签名、时间戳，成功后会在该知情同意类文书的相应位置显示签名人的电子签章。

具体实现流程如图 3.4 所示。

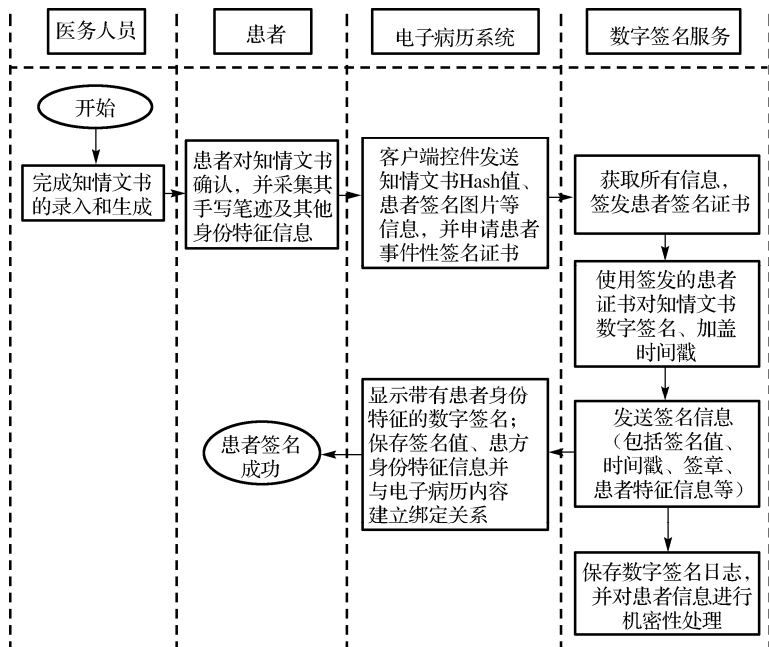


图 3.4 患者知情同意类文书确认数字签名实现流程图

患者知情同意类文书确认环节数字签名应用集成关键点主要包括以下三方面。

(1) 采集患者身份特征

通过手写签名板、摄像头、指纹仪等终端采集患者的身份特征信息，包括但不限于：手写签名、指纹、面部影像、身份证识别等，需采用两种或两种以上的特征。电子病历系统中存储的患者身份特征信息需与电子病历内容建立绑定关系。

(2) 签发患者数字证书

在医务人员鉴定过患者身份后，根据采集的患者身

份特征信息，为患者实时签发事件性数字证书。

(3) 患者手写数字签名

患者对知情同意类文书执行数字签名，同时加盖时间戳，并显示患者手写签名。

注：患者持有与医务人员相同的个人数字证书的，在知情同意类文书生成环节的数字签名实现方案可参照医务人员电子病历生成章节的数字签名实现方案实现。

3.3.4 电子病历归档环节

电子病历归档环节数字签名应用场景涉及电子病历管理部门、电子病历系统、电子病历归档系统、数字签名服务四类角色，其角色描述如表 3.4 所示。

表 3.4 电子病历归档环节数字签名应用场景角色描述

角 色	事 件 描 述
电子病历管理部门	归档电子病历数字签名主体，对已出院患者整份电子病历进行归档操作，对通过验证的电子病历执行数字签名
电子病历系统	调用数字签名验证接口、时间戳加盖及验证接口，发起对归档病历中数字签名及时间戳有效性的验证
电子病历归档系统	进行电子病历归档，发起对归档电子病历进行数字签名、加盖时间戳请求
数字签名服务	进行数字签名及验证、时间戳加盖及验证，并保存签名日志

电子病历归档环节中数字签名应用的具体实现流程如图 3.5 所示。

电子病历归档环节数字签名的关键点包括以下两方面。

(1) 电子病历归档前的数字签名有效性验证

通过签名验证接口验证电子病历内容的完整性、相关签名人数字证书的有效性及时间戳的有效性。

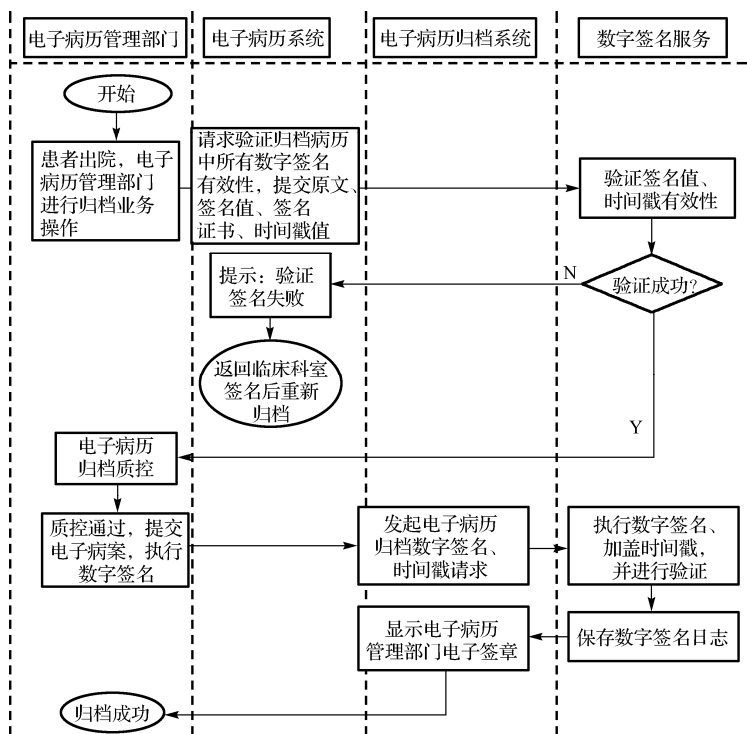


图 3.5 电子病历归档数字签名实现流程图

(2) 电子病历归档数字签名

电子病历管理部门对符合归档标准的电子病历向数字签名服务系统发起数字签名、时间戳请求，对电子病历执行数字签名、加盖时间戳。

3.3.5 电子病历复制环节

电子病历复制环节数字签名应用场景涉及电子病历管理部门、电子病历系统、数字签名服务三类角色，其角色描述如表 3.5 所示。

表 3.5 电子病历复制环节数字签名应用场景角色描述

角 色	事 件 描 述
电子病历 管理部门	电子病历复制环节数字签名主体，处理复制申请，对通过验证的复制部分电子病历执行数字签名
电子病历系统	调用数字签名验证接口、时间戳加盖及验证接口，发起对复制部分病历中数字签名及时间戳有效性验证，发起对通过验证的电子病历数字签名、加盖时间戳请求
数字签名服务	进行数字签名及验证、时间戳加盖及验证，并保存签名日志

电子病历复制环节中数字签名应用的具体实现流程如图 3.6 所示。

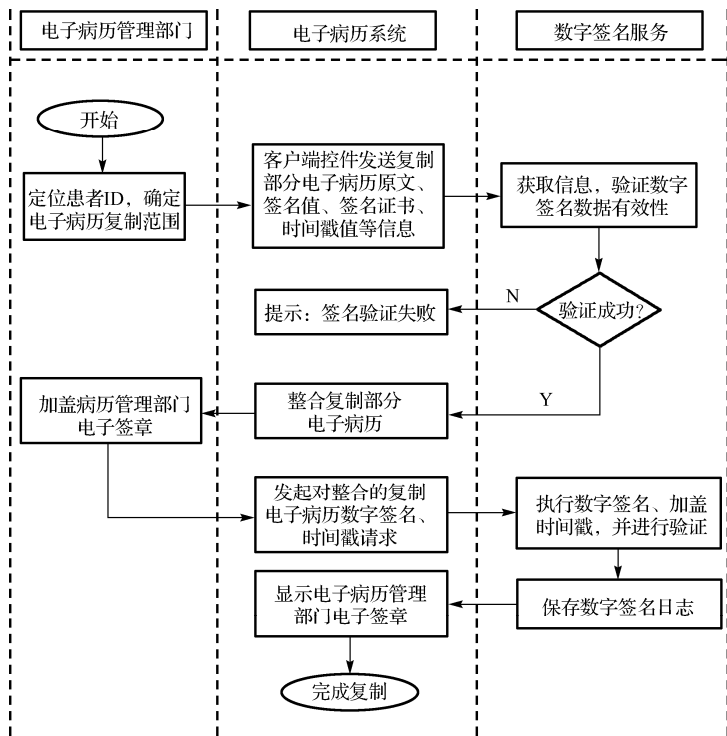


图 3.6 电子病历复制数字签名实现流程图

电子病历复制环节数字签名的关键点包括以下两方面。

(1) 电子病历复制部分内容数字签名数据有效性验证

相关医务人员确定复制内容，通过电子病历系统向数字签名服务系统发起数字签名数据有效性验证请求，对复制部分电子病历执行数字签名数据有效性的验证。

(2) 复制电子病历数字签名

医疗机构病历管理部门对已通过数字签名数据有效性验证的复制部分电子病历执行数字签名，加盖电子签章。

3.3.6 电子病历封存环节

电子病历封存环节数字签名应用场景涉及患者/代理人、电子病历管理部门/代理人、电子病历系统、数字签名服务四类角色，其角色描述如表 3.6 所示。

表 3.6 电子病历封存环节数字签名应用场景角色描述

角 色	事 件 描 述
患者/代理人	电子病历封存环节数字签名角色之一，提出封存申请，对通过验证的封存部分电子病历执行数字签名
电子病历管理部门/代理人	电子病历封存环节数字签名角色之一，处理封存申请，对通过验证的封存部分电子病历执行数字签名
电子病历系统	调用数字签名验证接口、时间戳验证接口，发起对封存部分病历中数字签名及时间戳有效性的验证，发起对通过验证的电子病历数字签名、加盖时间戳请求
数字签名服务	进行数字签名及验证、时间戳加盖及验证，并保存签名日志

电子病历封存时需先将需要封存的内容进行复制。封存环节数字签名应用的具体实现流程如图 3.7 所示。

电子病历封存环节数字签名的关键点包括以下三方面。

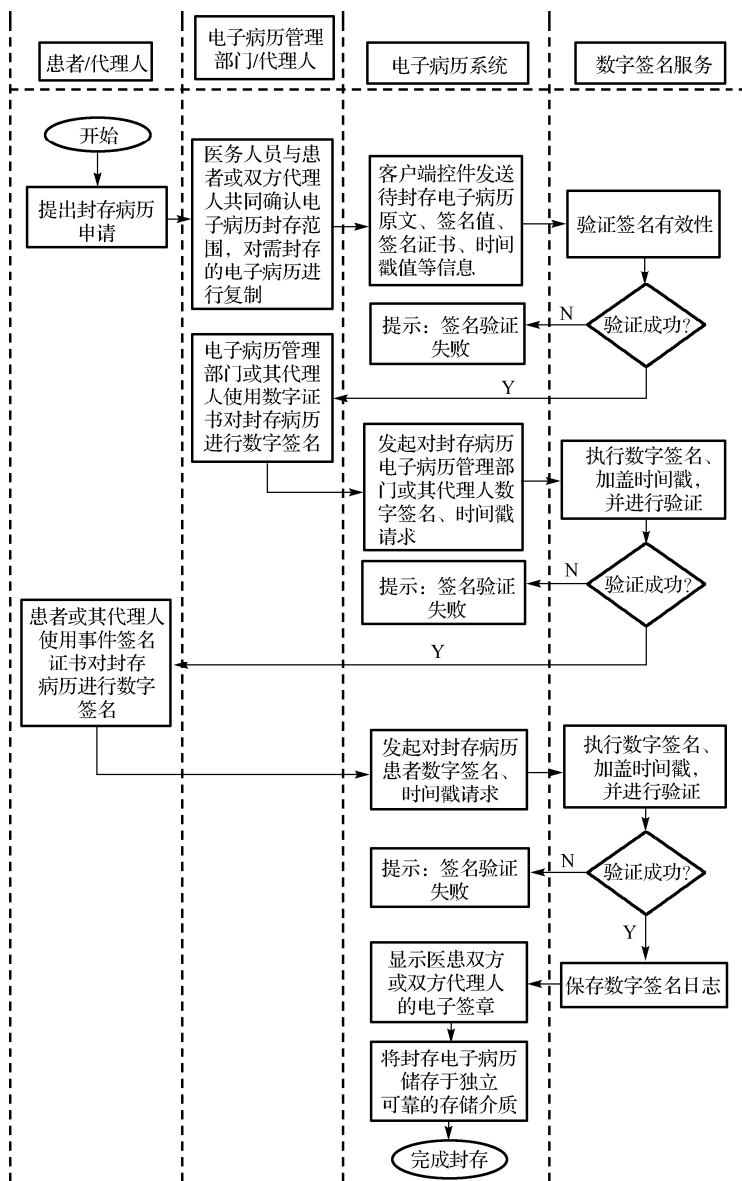


图 3.7 电子病历封存数字签名实现流程图

(1) 待封存电子病历内容数字签名数据有效性验证
医患双方或双方代理人共同确认封存电子病历范围，进行电子病历复制后通过调用签名验证接口，验证待封存电子病历数字签名的有效性。

(2) 医患双方数字签名
待封存电子病历签名验证通过后，医患双方分别执行数字签名。

(3) 保存封存电子病历
将经过医患双方或双方代理人数字签名的电子病历保存在独立可靠的存储介质中。

3.3.7 电子病历共享环节

电子病历共享环节数字签名应用场景涉及发送方和接收方两方面角色，发送方涉及发送单位、发送单位电子病历系统、发送方数字签名服务三类角色，其描述如表 3.7 所示。接收方涉及接收单位、接收单位电子病历系统、接收方数字签名服务三类角色，其描述如表 3.8 所示。

表 3.7 电子病历共享环节数字签名应用场景角色描述（发送方）

角 色	事 件 描 述
发送单位	共享电子病历的发送方，确定共享病历范围，对通过验证的共享部分电子病历执行数字签名
发送单位电子病历系统	调用数字签名验证接口、时间戳验证接口，发起对共享部分病历中数字签名及时间戳有效性的验证，发起对通过验证的电子病历数字签名、加盖时间戳请求
数字签名服务	进行数字签名及验证、时间戳加盖及验证，并保存签名日志

表 3.8 电子病历共享环节数字签名应用场景角色描述（接收方）

角 色	事 件 描 述
接收单位	共享电子病历的接收端
接收单位电子病历系统	调用数字签名验证接口、时间戳验证接口，发起对共享电子病历中数字签名及时间戳有效性的验证
数字签名服务	进行数字签名验证、时间戳验证

电子病历共享涉及发送医院与接收医院，发送方在共享电子病历前需执行数字签名及签名验证，接收方使用共享电子病历前需验证共享电子病历签名数据的有效性。其中数字签名及验证的实现方案同电子病历生成章节，电子病历共享过程中的数字签名可参考图 3.8 和图 3.9 执行操作。

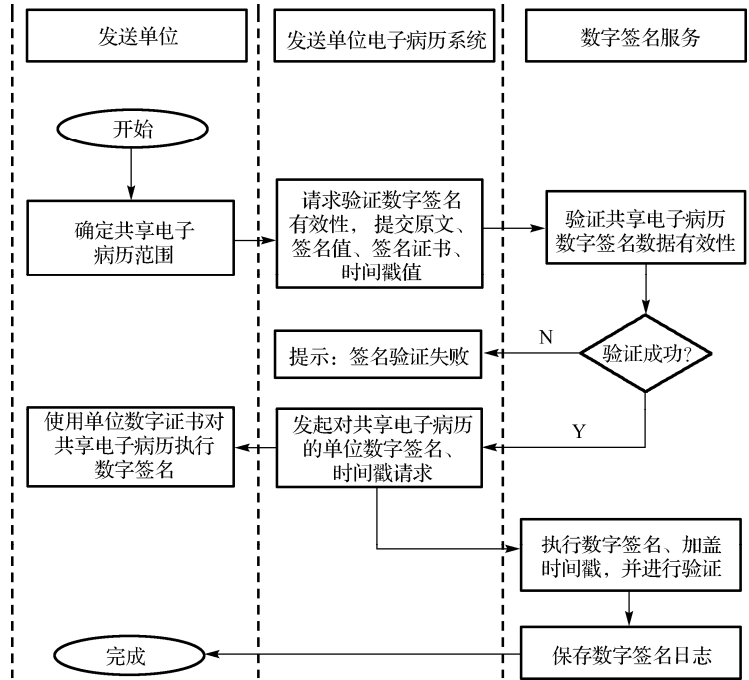


图 3.8 电子病历共享数字签名实现流程图（发送方）

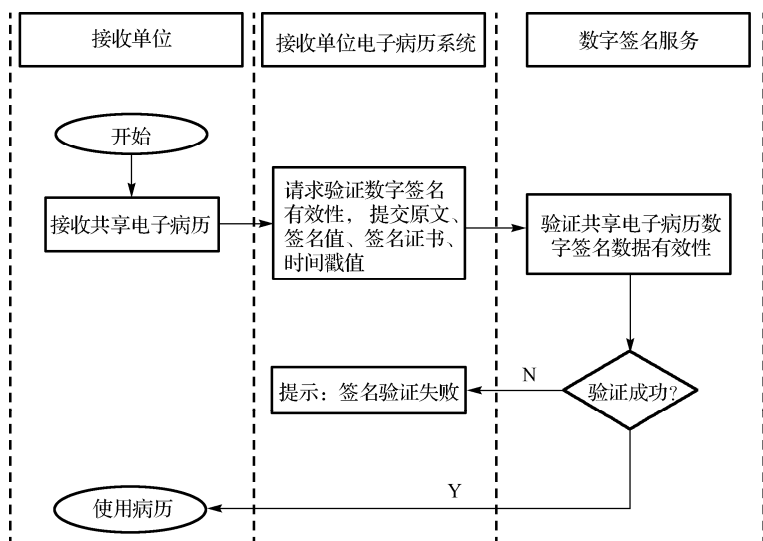


图 3.9 电子病历共享数字签名实现流程图（接收方）

电子病历共享环节数字签名的关键点包括以下两方面。

（1）发送单位对待共享电子病历进行数字签名及签名验证

发送单位选定共享电子病历，通过调用签名验证接口，验证待共享电子病历数字签名数据的有效性，验证通过后对共享电子病历执行数字签名及签名验证。

（2）接收单位验证共享电子病历数字签名数据的有效性

接收单位在接收共享电子病历时对电子病历进行签名有效性验证，验证通过后使用电子病历。

4

电子病历数字签名数据结构

4.1 带数字签名电子病历的构成

电子病历文档采用开放格式存储，如 HTML、纯文本及 XML 等，其中 XML 为最常用的国际标准文档格式。以电子病历数字签名数据结构 XML 表述为例，在保存数字签名时要确保数字签名数据与电子病历一一对应的关联关系，电子病历与其数字签名数据关联关系如图 4.1 所示。

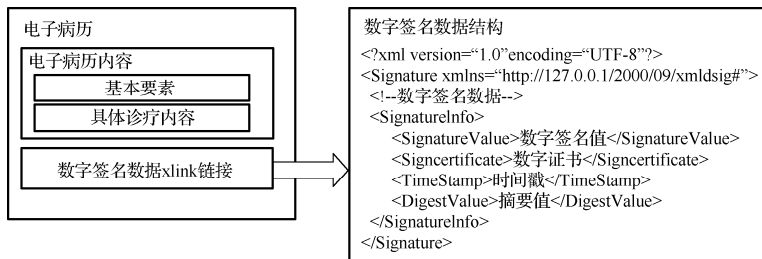


图 4.1 电子病历数字签名数据关联关系

4.2 电子病历内容要求

电子病历及其数字签名数据结构 XML 文档中，电子病历作为数字签名的原文，其内容需要包括基本要素、具体诊疗内容等，具体内容如下。

（1）基本要素（Clinical Base Doc Element）：主要标识患者就诊过程中产生的唯一诊疗记录。通过基本要素中的信息可查询和定位患者在某医院中的某条就诊信息。主要包括：病人唯一标识码、患者就诊门诊号、患者就诊住院号、医院组织机构代码、执行人识别信息、就诊日期、就诊次、就诊类型（门急诊、住院等）、病历文档唯一标识码、病历文档类别（病案首页、入院记录、病程记录等）、文档版本号码（所生成 XML 文档的版本号）。

（2）具体诊疗内容（Encompassing Encounter Content）：记录患者某次就诊过程中所产生的具体诊疗的文字性内容。该部分主要可了解患者本次就诊中某一类型病历文书的诊疗经过和描述。该部分内容参考附录 A “数字签名诊疗数据要素” 所要求内容。

4.3 数字签名数据要求

在数字签名数据结构 XML 文档中，需要包括的具体内容如下。**数字签名数据（SignatureInfo）：**记录患者某次就诊所产生某一类型电子病历文书的数字签名相关

信息，该 XML 文件与所签的电子病历 XML 文件进行关联，主要包括签名值、数字证书、时间戳值、Hash 值等。

数字签名数据格式应采用符合 GB/T 25064《信息安全技术 公钥基础设施 电子签名格式规范》要求的带时间戳的电子签名（ES-T）。具体说明如表 4.1～表 4.4 所示。

表 4.1 SignatureInfo. SignatureValue 说明

节 点 名 称	类 型	定 义	说 明
SignatureValue	字 符	签名值	数字签名后产生的签名数据，标识原文信息的真实可信

表 4.2 SignatureInfo. Signcertificate 说明

节 点 名 称	类 型	定 义	说 明
Signcertificate	字 符	数字证书	标识签名人的可靠数字身份，并用于验证签名的有效性

表 4.3 SignatureInfo. TimeStamp 说明

节 点 名 称	类 型	定 义	说 明
TimeStamp	字 符	时间戳	标识签名时间的真实可信

表 4.4 SignatureInfo. Hash 说明

节 点 名 称	类 型	定 义	说 明
Hash	字 符	Hash 值	标识原文的摘要值，用于数字签名及签名验证

4.4

数字签名示例

以检验报告单为例。

门诊

检验报告单

项目名称: 乙肝五项(快速发光定量法)样本编号: MD0647

姓名: 李杉性别: 女年龄: 27岁标本类型: 血采集时间: 2018-3-13 10:15备注:

科室: 中医科门诊病历号: A101597943床号: 临床诊断: 申请医生: 刘淑刚

编码	项目名称	结果	参考区间	单位
IHBsAg	☆乙型肝炎病毒表面抗原	0.600-	<1	COI
IHBsAb	☆乙型肝炎病毒表面抗体	2.000-	<10	IU/L
IHBcAg	乙型肝炎病毒e抗原	0.099-	<1	COI
IHBcAb	乙型肝炎病毒e抗体	1.340-	>1	COI
IHBcAb	乙型肝炎病毒核心抗体	0.009+	>1	COI

接收时间: 2018-03-13 11:06报告时间: 2018-03-13 14:04检验者: 满宏伟审核者: 郭亚阳

实验室名称: 检验科免疫科

电子病历 XML 数据结构示例如下。

```
<?xml version = "1.0" encoding = "uft-8"?>
<ClinicalDocument xmlns="urn:hl7-org:v3"
xmlns:xlink="http://www.w3.org/1999/xlink">
  <ClinicalDocumentElement>
    <!-- 基本要素 -->
    <ClinicalBaseDocElement>
      <EncompassingEncounterType>门诊</Encompassing-
        EncounterType>--就诊类型
      <ProjectName>乙肝五项(快速发光定量法)</ProjectName>--项目名称
      <SampleNumber>MD0674</SampleNumber>--样品编号
      <PatientName>李杉</PatientName>--患者姓名
      <PatientSex>女</PatientName>--患者性别
      <PatientAge>27岁</PatientName>--患者年龄
      <SpecimenSpecies>血</SpecimenSpecies>--标本类型
      <SamplingDate>2018-3-13 10:15</SamplingDate>--采样时间
      <Remarks></Remarks>--备注
      <ApplicationDepartment>中医科门诊</Application- Department>--申请科室
      <PatientId>A101597943</PatientId>--病历号
      <BedNum></BedNum>--床号
      <ClinicalDiagnosis></ClinicalDiagnosis>--临床诊断
      <ApplicationDoctor>刘淑刚<ApplyDoctor>--申请医生
```



```

        <ReceivingTime>2018-03-13 11:06</ReceivingTime>--接收时间
        <ReportingTime>2018-03-13 14:04</ReportingTime>--报告时间
        <Rapporteur>满宏伟</Rapporteur>--检验者
        <Proofreader>郭亚阳</Proofreader>--审核者
        <LaboratoryName>检验科免疫组<LaboratoryName/>--实验室名称
    </ClinicalBaseDocElement>

    <!-- 具体诊疗内容 -->

    <EncompassingEncounterContent>--mygyy|1|A101597943|李杉|2|27 岁
|2409|A0709|2018-03-13 14:04|1|HBCAB, 0.009|HBEAB- B, 1.340|HBEAG-B,
0.099|HBSAB-B, 2.000|HBSAG-B, 0.600
    </EncompassingEncounterContent>

    <!--数字签名数据关联路径-->

    <Description
Xlink:type="simple"
Xlink:href="...../Signature"> --数字签名数据存放路径
    </Description>>

    </ClinicalDocumentElement>

```

对应的数字签名数据 XML 数据结构示例如下。

在应用本书存放数字签名数据时,需将 GB/T 25061《信息安全技术 公钥基础设施 XML 数字签名语法与处理规范》中的附录文件存放在电子病历系统中可以访问的位置,本书中假定存放在 <http://127.0.0.1/2000/09/xmldsig>,可根据实际情况调整存放位置,关联的数字签名 XML 数据结构示例如下。

```

<?xml version = "1.0" encoding = "uft-8"?>
<Signature xmlns="http://127.0.0.1/2000/09/xmldsig#">
<!-- 数字签名数据 -->
    <SignatureInfo>
    <SignatureValue>--签名值
qmZYS5d8FpsJh+owwyeMgNTUGdUYZM6l1FzJ41LUv4icEEFPXgOibv
2gJJmrXprgaCfzaHogHyJanLBkl/h7/GmMM91qcANerG7LAvCJ6yA7oDkXpV
apU6NcCxocln9DEyk6QJbFv0pGWChQs4KlpcuxoHMiSWF4L/ivY+YVV38=
    </SignatureValue>

```

<Signcertificate>--数字证书

MIIFczCCBFugAwIBAgIKGzAAAAAAAAAAZImjANBgkqhkiG9w0BAQUF
ADBSMQswCQYDVQQGEwJDTjENMAsgA1UECgwEQkpDQTEYMBYGA1U
ECwwPUHVibGljIFRydXN0IENBMRowGAYDVQQDDBFQdWJsaWMgVHJlc3
QgQ0EtMTAeFw0xNTA2.....

</Signcertificate>

<TimeStamp>--时间戳值

MIICGQYJKoZIhvcNAQcCoIICCjCCAgYCAQMxCzAJBgUrDgMCGGU
AMFsGCyqGSIb3DQEJEAEEoEwESjBIAgEBBgEqMCEwCQYFKw4DAhoFA
AQUPxIs7ALq4V3jsmLNI3Jam8Os894CBAX14QEYDzIwMTcwMjI3MDI1ND
E5WgIGAVp9fXqVMYIBITCCA.....

</TimeStamp>

<Hash>--Hash 值

PxIs7ALq4V3jsmLNI3Jam8Os894=.....

</Hash>

</SignatureInfo>

</Signature>

5

数字签名数据存储与访问

5.1 数字签名数据的存储

数字签名数据在医院信息系统的数据库中有两种存储方式：一种是集中存储，另一种是分散存储。集中存储是指医院内各类信息系统产生的签名数据、签名日志统一存放在一个指定的数据库，它的优势是签名数据容易备份、整体性操作简单，但是对医院各类信息系统的程序调整比较多、数据管理复杂；分散存储是指医院各类信息系统存储各自产生的签名数据和签名日志，它的优势是数据完整、易分离、易存储，同时信息系统的程序改动少。这里一般建议医院采用分散存储，便于签名数据在司法鉴定时能够完整地得到。

数字签名数据除在医院各类信息系统中存储外，还需要在签名验证系统中存储数字签名日志，确保数字签名数据真实完整。

5.1.1 运行中的电子病历及其数字签名存储

(1) 经数字签名验证通过的电子病历及其数字签名

数据，在电子病历系统数据库中需建立关联关系，分别存储。

（2）在条件允许的情况下，建议在脱离电子病历系统的存储环境中备份存储电子病历及其数字签名数据，以确保数据的安全性。

（3）独立存储数字签名日志，存储内容包括数字签名流水号、原文的唯一序列号、患者唯一标识、患者姓名、签名人姓名、电子病历原文 Hash 值、数字签名值、时间戳值、签名人数字证书等信息。

（4）保存的数字签名要满足司法举证的要求，能够验证电子病历的真实性、完整性。

5.1.2 归档后的电子病历及其数字签名存储

电子病历归档后，要在脱离电子病历系统的存储环境中存储电子病历及其数字签名数据，且存储内容能够通过数字签名验证，确保归档电子病历真实完整、合法可信。

5.2 存储数据的访问

访问存储数据时，需对访问者进行身份认证，实现方案可参考医务人员身份认证章节。

在独立存储电子病历数字签名日志的数字签名服务系统中，可以通过患者唯一标识、医生信息等关键字进行查询、访问相关数据，并可导出作为医疗纠纷司法鉴定的举证材料。

6

数字证书服务

6.1 数字证书服务内容

由第三方电子认证服务机构面向医务人员证书用户提供符合《卫生系统电子认证服务规范（试行）》的数字证书全生命周期服务，包括证书申请、证书更新、证书吊销、证书载体解锁、证书重签发等。传统的数字证书一般以 **USB Key** 为载体，随着科技的发展，以手机作为数字证书载体的应用将越来越广泛，无论数字证书采用何种载体，数字证书的服务内容相同，不同的是服务形式，手机模式的证书服务可通过手机端的证书管理应用来自助完成，以下主要介绍以 **USB Key** 为证书载体的证书服务模式。

具体数字证书服务内容如下。

（1）证书申请

证书申请者到医院证书受理点申请证书，由证书受理点管理员根据证书申请用户所提供的证明材料，对用户的身份进行审核，并为通过审核的用户签发证书。

（2）证书更新

证书有效期为一年，医务人员证书到期后，需要进行更新操作。医务人员可到证书受理点进行办理，由管理员在进行身份审核后进行医务人员证书的更新操作，还可以基于证书服务系统实现自动更新的方式，在医院与第三方电子认证服务机构确认证书更新用户信息后，由第三方电子认证服务机构为医务人员签发证书更新授权，管理员需进行年度一次性的授权文件导入操作，完成本医院所有证书用户的证书更新工作，证书用户在正常登录医院各类信息系统后，可实现证书自动更新。

（3）证书吊销

由于密钥遗失、人员变动或其他原因，在证书用户提出吊销申请后，管理员废除该指定用户的证书，并通过第三方电子认证服务机构的证书签发系统进行作废证书列表的发布，使该证书不能再次使用。

（4）证书载体解锁

证书用户由于遗忘或输错证书保护 PIN 码导致证书锁定，可到证书受理点申请解锁，受理点管理员核实证书用户身份后，可进行载体解锁。

（5）证书重签发

当医务人员证书载体损坏时，可到证书受理点申请重新签发证书，受理点管理员核实用户身份后重新为用户签发证书。

6.2 数字证书服务模式

为保证数字证书服务及时可达和医院管理自主化，

建议在医院内部建设证书受理点，并由医院指定证书管理员，为医务人员等内部工作人员发放、更新个人数字证书。

医院内部初次申请签发数字证书时，可采用批量申请模式，由医院证书受理点收集并确认所有证书用户的个人信息，再交由第三方电子认证服务机构集中制作数字证书，将制作完成的载有数字证书的介质送至医院，由证书管理员将证书发放给证书用户。

在医院批量证书制作发放完毕后，如遇到医务人员入职或其他人员流动，需办理零散用户的证书申请业务时，可由医院证书管理员通过证书受理点自助制作和发放数字证书，第三方电子认证服务机构在后台签发数字证书。

7

电子病历数字签名系统建设实施过程

7.1 电子病历数字签名的实施条件

以医院电子病历系统为核心，建立医院统一的电子认证服务体系，需要医院信息化建设满足以下实施条件。

(1) 医院实施电子病历数字签名需要医院领导的全力支持和相关业务部门的配合。

(2) 具有专门的技术支持部门和人员，负责电子病历相关信息系统建设、运行和维护等工作；具有专门的管理部门和人员，负责电子病历的业务监管等工作；具有专职人员负责数字签名系统的实施及数字证书的日常工作，包括数字证书的签发、更新、吊销、丢失补办、证书介质解锁等。

(3) 医院已建立比较完善的电子病历相关信息系统，如 LIS 系统、PACS 系统、HIS 系统等。

7.2 电子病历数字签名的实施步骤

在建设数字签名系统之前，从全院整体角度做好规

划是一项重要的工作。在这个规划中，要明确电子病历数字签名实施的所有步骤。

（1）医院成立数字签名系统建设的领导组织机构、工作组织机构，明确技术部门、相关业务部门的职责和任务。

（2）了解电子病历相关信息系统建设现状、数字签名的需求，对实施数字签名进行前期评估，制订数字签名系统实施方案和实施计划。

（3）建立数字签名有关的管理制度，包括数字证书发放和使用管理制度、数字签名操作业务流程规范等。

（4）按照国家有关要求，如《卫生系统电子认证服务管理办法（试行）》等，选择合适的第三方电子认证服务机构。

（5）数字签名系统实施。

① 数字签名系统的硬件准备。签名验证服务器、时间戳服务器、证书管理服务器等设备的到货、上架安装、调试。

② 数字签名系统与医院信息系统集成。根据系统建设现状和数字签名需求，集成范围包括：电子病历系统、HIS 系统、LIS 系统、PACS 系统、归档系统的证书注册、登录认证、数字签名及验证、时间戳、电子签章等集成工作。

③ 进行集成测试。要点包含：电子病历系统、HIS 系统、LIS 系统、PACS 系统、归档系统的证书注册、登录认证、数字签名及验证、时间戳、电子签章的相关测试。测试通过后，医院方、第三方电子认证服务提供方

共同签署《产品集成与测试报告》及《业务系统数字签名功能测试》，模板如表 7.1 和表 7.2 所示。

表 7.1 产品集成与测试报告

项 目 名 称			
建 设 方			
承 建 方			
最 终 用 户			
实 施 人 员		实 施 时 间	
业务系统名称		开 发 语 言	
系统开发商			
开发商联系人		电 话	
系统集成电子 认证功能点			
数字签名系统硬件设备部署信息			
产 品	IP 地 址	端 口	

表 7.2 业务系统数字签名功能测试

测 试 项	测试步骤（方法）	预 期 效 果	测 试 结 果
1			[]符 合 []不符合
2			[]符 合 []不符合
3			[]符 合 []不符合
4			[]符 合 []不符合
5			[]符 合 []不符合
用户代表签字： 日 期：		承建方签字： 日 期：	

④ 证书服务。医院医护/医技人员的信息收集、手写

签章采集、数字证书制作、数字证书发放、受理点建设、证书生命周期服务等。

⑤ 运行准备工作。组织人员进行“证书环境”安装工作。明确证书管理员，进行证书受理点的日常工作，包括发证、吊销、丢失补办、证书介质解锁等。

⑥ 人员培训。包括数字签名验证服务系统维护人员培训、证书管理员培训、医务人员的数字签名相关业务操作培训等。

⑦ 试运行。选择 2~3 个临床科室，依次对每个系统进行数字签名应用试运行。

⑧ 正式运行。全院系统逐个全面实施数字签名。

(6) 数字签名系统建设完成后，按照信息化项目验收规范对项目进行验收。

7.3 实施数字签名的培训内容

医院数字签名项目培训的对象，主要包括本项目涉及的信息系统开发商、证书管理员、系统管理员、医院数字证书使用者四类。

培训内容包括以下几方面。

(1) 针对医院信息系统开发商的接口对接、签名验证等技术培训。

(2) 证书管理员日常证书管理工作的培训，主要是培训数字证书在线服务平台的操作功能，包括证书在线申请、证书更新、证书注销、证书查询、证书介质解锁等操作。

(3) 系统管理员培训主要是数字签名服务系统使用培训，包括对数字签名服务系统使用及维护培训，使其能排除一般性故障，保证系统日常运行。

(4) 医院数字证书使用者培训，主要是日常数字签名操作培训，包括提供数字证书产品的业务操作、使用流程、注意事项方面的培训。

7.4 数字证书发放的部门、人员

数字证书发放部门：临床科室、医技科室、病案管理部门等。

数字证书发放人员：具有执业资格的临床科室医生、护士、检验科检验师、检查报告审核医师等医疗卫生人员、医务处等管理部门相关管理人员、信息技术支持人员。

7.5 需进行数字签名的病历文书

(1) 门（急）诊病历数字签名清单：门（急）诊病历首页、门（急）诊病历记录、急诊留观记录、门诊处方、门诊检验报告单、门诊辅助检查报告单。

(2) 住院病历数字签名清单：住院病案首页、24 小时入出院记录、24 小时入院死亡记录、入院记录、病程记录（首次病程记录、日常病程记录、上级医师查房记录、疑难病例讨论记录、交班记录、接班记录、转入记录、转出记录、阶段小结、抢救记录、有创诊疗操作记录、会诊申请、会诊意见记录、术前小结、术前讨论记

录、麻醉术前访视记录、麻醉记录、手术记录、手术安全核查记录、手术清点记录、术后首次病程记录、麻醉术后访视记录)、出院记录、死亡记录、死亡病例讨论记录、病重(危)患者护理记录、手术同意书、麻醉同意书、输血治疗知情同意书、授权委托书、特殊检查、特殊治疗同意书、病危(重)通知书、医嘱单、体温单、检验报告单、辅助检查报告单。

7.6 数字签名实施的注意事项

(1) 实施数字签名要得到医院领导的支持和业务部门的配合。

(2) 与不同信息系统的对接一定要针对不同数据,采取不同的数字签名及验证方式。

(3) 对每一次数字签名要进行验证,以确保其有效性。

(4) 数字签名实施以不影响医院现有应用系统的正常运行为前提。

(5) 实施数字签名在一定程度上会改变医务人员现有的操作流程,应尽量以使现有流程更便捷、舒畅为原则来实施。

(6) 系统建设必须符合相关法律法规的要求。

附录 A 数字签名诊疗数据要素

（资料性附录）

1. 门（急）诊病历数字签名诊疗数据要素

数字签名需要至少实现对这些数据项内容的保护。

1) 门（急）诊病历首页

病人唯一标识码、患者姓名、性别、出生年月日、民族、婚姻状况、职业、工作单位、住址、药物过敏史、建立门（急）诊病历首页时间。

数字签名执行人：医师。

2) 门（急）诊病历记录

病人唯一标识码、就诊时间、科别、主诉、现病史、既往史、查体、辅助检查结果、诊断、处理意见、就诊时间。

数字签名执行人：医师。

3) 急诊留观记录

病人唯一标识码、患者姓名、性别、年龄、职业、留观记录内容、留观记录时间。

数字签名执行人：医师。

4) 门诊处方

病人唯一标识码、患者姓名、科别、诊断、处方内容[详见《处方管理办法》（卫生部第 53 号令）中处方标准内容]、处方日期。

数字签名执行人：医师。

5) 门诊检验报告单

病人唯一标识码、姓名、性别、年龄、检验项目、检验结果、报告日期。

数字签名执行人：检验医师、审核医师。

6) 门诊辅助检查报告单

病人唯一标识码、姓名、性别、年龄、辅助检查项目、辅助检查描述、辅助检查结果、报告日期。

数字签名执行人：检查医师、审核医师。

2. 住院病历数字签名诊疗数据要素

数字签名需要至少实现对这些数据项内容的保护。

1) 住院病案首页及中医住院病案首页

内容参照国家卫生健康委员会统计调查制度。

数字签名执行人：科主任、主任（副主任）医师、主治医师、住院医师、编码员。

2) 24 小时入出院记录

病人唯一标识码、患者姓名、性别、年龄、职业、入院时间、出院时间、主诉、入院情况、入院诊断、诊疗经过、出院情况、出院诊断、出院医嘱。

数字签名执行人：经治医师。

3) 24 小时入院死亡记录

病人唯一标识码、患者姓名、性别、年龄、职业、入院时间、死亡时间、主诉、入院情况、入院诊断、诊疗经过（抢救经过）、死亡原因、死亡诊断。

数字签名执行人：经治医师。

4) 入院记录

病人唯一标识码、患者一般情况、主诉、现病史、既往史、个人史、婚育史、家族史、体格检查、专科情况、辅助检查、初步诊断。

数字签名执行人：医师。

5) 病程记录

(1) 首次病程记录：病人唯一标识码、患者姓名、病例特点、拟诊讨论（诊断依据及鉴别诊断）、诊疗计划。

数字签名执行人：医师。

(2) 日常病程记录：病人唯一标识码、患者姓名、诊疗内容。

数字签名执行人：经治医师。

(3) 上级医师查房记录：病人唯一标识码、患者姓名、查房医师姓名和专业技术职务、查房意见。

数字签名执行人：医师。

(4) 疑难病例讨论记录：病人唯一标识码、患者姓名、讨论日期、主持人、参加人员姓名和专业技术职务、具体讨论意见及主持人小结意见。

数字签名执行人：医师。

(5) 交班记录：病人唯一标识码、患者姓名、入院日期、交班日期、主诉、入院情况、入院诊断、诊疗经过、目前情况、目前诊断、交班注意事项。

数字签名执行人：交班医师。

(6) 接班记录：病人唯一标识码、患者姓名、性别、年龄、入院日期、接班日期、主诉、入院情况、入院诊断、诊疗经过、目前情况、目前诊断、接班诊疗计划。

数字签名执行人：接班医师。

(7) 转入记录：病人唯一标识码、患者姓名、性别、年龄、入院日期、转入日期、转入科室、主诉、入院情况、入院诊断、诊疗经过、目前情况、目前诊断、转入诊疗计划。

数字签名执行人：转入科室医师。

(8) 转出记录：病人唯一标识码、患者姓名、性别、年龄、入院日期、转出日期，转出科室、入院情况、入院诊断、诊疗经过、目前情况、目前诊断、转科目的及注意事项。

数字签名执行人：转出科室医师。

(9) 阶段小结：病人唯一标识码、患者姓名、性别、年龄、入院日期、小结日期、主诉、入院情况、入院诊断、诊疗经过、目前情况、目前诊断、诊疗计划。

数字签名执行人：经治医师。

(10) 抢救记录：病人唯一标识码、患者姓名、病情变化情况、抢救措施、参加抢救人员的姓名和专业技术职称。

数字签名执行人：参加抢救人员。

(11) 有创诊疗操作记录：病人唯一标识码、患者姓名、操作名称、操作时间、操作过程记录。

数字签名执行人：医师。

(12) 会诊申请：病人唯一标识码、患者姓名、会诊申请科室、会诊申请时间、会诊申请理由。

数字签名执行人：医师。

(13) 会诊意见记录：病人唯一标识码、患者姓名、会诊科室、会诊意见、会诊时间。

数字签名执行人：医师。

（14）术前小结：病人唯一标识码、患者姓名、简要病情、术前诊断、手术指征、拟施手术名称、拟施手术方式、拟施麻醉方式、注意事项。

数字签名执行人：经治医师。

（15）术前讨论记录：病人唯一标识码、患者姓名、参加讨论者的姓名和专业技术职务、具体讨论意见、主持人小结意见、讨论日期。

数字签名执行人：医师。

（16）麻醉术前访视记录：病人唯一标识码、患者姓名、性别、年龄、科别、病案号、患者一般情况、访视内容记录。

数字签名执行人：麻醉医师。

（17）麻醉记录：病人唯一标识码、患者一般情况、术前特殊情况、麻醉前用药、术前诊断、术中诊断、手术方式及日期、麻醉方式、麻醉诱导、各项操作开始及结束时间、麻醉期间用药名称、方式及剂量、麻醉期间特殊或突发情况、麻醉期间特殊或突发情况处理、手术起止时间。

数字签名执行人：麻醉医师。

（18）手术记录：病人唯一标识码、患者姓名、性别、年龄、科别、病房、床位号、住院病历号（或病案号）、手术日期、术前诊断、术中诊断、手术名称、麻醉方法、手术经过。

数字签名执行人：手术医师。

（19）手术安全核查记录：病人唯一标识码、患者姓

名、麻醉开始前核查内容、手术开始前核查记录内容、出手术室前核查记录内容。

数字签名执行人：手术医师、麻醉医师、手术护士。

(20) 手术清点记录：病人唯一标识码、患者姓名、住院病历号（或病案号）、手术日期、手术名称、术中所用各种器械和敷料数量的清点核对。

数字签名执行人：巡回护士、手术器械护士。

(21) 术后首次病程记录：病人唯一标识码、患者姓名、术后病程记录。

数字签名执行人：医师。

(22) 麻醉术后访视记录：病人唯一标识码、患者姓名、性别、年龄、科别、住院病历号（或病案号）、患者一般情况、术后访视记录。

数字签名执行人：麻醉医师。

6) 出院记录

病人唯一标识码、患者姓名、性别、年龄、出院日期、入院情况、入院诊断、诊疗经过、出院诊断、出院情况、出院医嘱。

数字签名执行人：医师。

7) 死亡记录

病人唯一标识码、患者姓名、性别、年龄、入院日期、死亡时间、入院情况、入院诊断、诊疗经过（包括抢救经过）、死亡原因、死亡诊断。

数字签名执行人：医师。

8) 死亡病例讨论记录

病人唯一标识码、患者姓名、讨论日期、主持人和

职务、参加人员姓名和专业技术职务、具体讨论意见、主持人小结意见。

数字签名执行人：医师。

9) 病重（危）患者护理记录

病人唯一标识码、患者姓名、性别、年龄、科别、住院病历号（或病案号）、床位号、页码、记录日期和时间、护理记录内容。

数字签名执行人：护士。

10) 手术同意书

病人唯一标识码、患者姓名、术前诊断、手术名称、手术风险、替代医疗方案、患方意见。

数字签名执行人：医师、患方。

11) 麻醉同意书

病人唯一标识码、患者姓名、性别、年龄、科别、住院病历号（或病案号）、术前诊断、拟行手术方式、拟行麻醉方式、麻醉风险、患方意见。

数字签名执行人：麻醉医师、患方。

12) 输血治疗知情同意书

病人唯一标识码、患者姓名、性别、年龄、科别、住院病历号（或病案号）、诊断、输血指征、拟输血成分、输血风险、患方意见。

数字签名执行人：医师、患方。

13) 授权委托书

病人唯一标识码、患者姓名、性别、年龄、科室、住院病历号（或病案号）、诊断、授权委托内容。

数字签名执行人：患者、被委托人、医师。

14) 特殊检查、特殊治疗同意书

病人唯一标识码、患者姓名、术前诊断、特殊检查、特殊治疗名称、特殊检查、特殊治疗风险、替代医疗方案、患方意见。

数字签名执行人：医师、患方。

15) 病危（重）通知书

病人唯一标识码、患者姓名、性别、年龄、科别、目前诊断、病危情况通报。

数字签名执行人：医师、患方。

16) 医嘱单

(1) 长期医嘱单：病人唯一标识码、患者姓名、科别、住院病历号（或病案号）、长期医嘱起始日期和时间、长期医嘱内容、长期医嘱停止日期和时间、执行时间。

数字签名执行人：医师、执行护士。

(2) 临时医嘱单：病人唯一标识码、患者姓名、科别、住院病历号（或病案号）、临时医嘱日期和时间、临时医嘱内容、执行时间。

数字签名执行人：医师、执行护士。

17) 体温单

病人唯一标识码、患者姓名、科别、住院病历号（或病案号）、床号、入院日期、手术后天数、体温、脉搏、呼吸、血压、大便次数、出入液量、体重。

数字签名执行人：护士。

18) 检验报告单

病人唯一标识码、患者姓名、性别、年龄、病历号（或病案号）、检验项目、检验结果、报告日期。

数字签名执行人：检验医师、审核医师。

19) 辅助检查报告单

病人唯一标识码、患者姓名、性别、年龄、住院病历号（或病案号）、辅助检查项目、辅助检查描述、辅助检查结果、报告日期。

数字签名执行人：检查医师、审核医师。

附录 B 数字签名应用集成实例

（资料性附录）

本实例以 LIS 系统检验报告为例。

1. 环境准备

- （1）数字签名服务产品到货、上架并安装调试；
- （2）第三方电子认证服务提供商与医院信息系统开发商、医院方确认集成方案，并发送相应的集成资料；
- （3）收集医护人员的证书信息和手写签名，将数字证书和电子签章图片录 USB Key 中；
- （4）医院各科室电脑端安装数字签名客户端。

2. 数字签名应用集成步骤

1) 数字证书与医院信息系统账户绑定

- （1）调用证书用户列表获取接口，得到证书操作唯一标识，即介质序列号+密码卡序列号；
- （2）通过证书操作唯一标识，调用用户证书导出接口，得到用户数字证书；
- （3）调用证书唯一标识获取接口，得到数字证书唯一标识，即“SF+身份证号”，将证书唯一标识保存到信息系统数据库的系统用户表中。用户表具体改造如表 B.1 所示。

表 B.1 信息系统数据库改造用户表示意图

登录名	密码	姓名	职务	电子签章	证书用户唯一标识
lvweihua	XXXX	吕伟华	主任	! # ¥ % … … &	SF152225198209270056

2) 身份认证

(1) LIS 系统服务端调用随机数接口，得到一个随机数，随机数通过 session 对象返回给签名验证系统客户端；

(2) LIS 系统调用签名验证系统客户端组件，在登录页面显示所有数字证书的用户名。选择对应的数字证书，输入 PIN 码，通过 LIS 系统程序验证 PIN 码是否正确；

(3) 如果 PIN 码正确，会触发签名验证系统客户端使用医务人员的私钥，对随机数进行签名，并将签名后生产的签名值及数字证书发送给签名验证系统服务端；

(4) 签名验证系统服务端调用签名验证接口对医务人员数字证书和签名值进行验证，验证通过后签名验证服务端解析证书信息，获取“证书用户唯一标识”，并与 LIS 系统数据库比对，比对成功则登录成功。

3) 签名、加盖时间戳

在 LIS 系统的关键业务节点的提交功能中添加签名和加盖时间戳功能，签名完成后保存相应数据，即需要修改业务系统数据表，增加证书信息、Hash 值、签名值、时间戳值四个字段，用于保存证书值、Hash 值、签名值、时间戳值。具体流程如下。

(1) 获取签名原文，签名原文是由医院 LIS 系统开发商根据检验报告的展示规则提供的 XML；

(2) LIS 系统调用电子签章系统签章图片获取控件获取电子签章图片，返回图片的 base64 编码；

(3) LIS 系统调用数字签名组件的签名接口对原文进行数字签名，然后将电子签章图片放到检验报告的固定位置；

(4) LIS 系统调用时间戳系统接口，对签名原文和图片加盖时间戳。

4) 验证签名数据和时间戳数据

从 LIS 系统数据库中取得证书信息、签名原文、签名值、时间戳值，调用验证接口判断信息是否正确，具体流程如下。

(1) LIS 系统调用组件，获取数字签名与时间戳相关信息；

(2) LIS 系统调用签名验证系统组件接口，验证数字签名值；

(3) 调用时间戳组件接口，验证时间戳服务。

5) 保存数字签名日志

签名数据验证通过后，调用保存签名日志接口，保存日志。日志信息应包括：数字签名流水号、数字签名对象的唯一序列号、患者姓名、签名人姓名、原文 Hash 值、数字签名、时间戳、签名人数字证书。

6) 检查与测试

LIS 系统与数字签名系统集成完后，需要按照第三方电子认证服务机构的要求进行系统测试。

3. 签名原文实例

```
<?xml version = "1.0" encoding = "uft-8" ?>
```

```

<ClinicalDocument xmlns="urn:hl7-org:v3"
xmlns:xlink="http://www.w3.org/1999/xlink">
  <ClinicalDocumentElement>
    <!-- 基本要素 -->
    <ClinicalBaseDocElement>
      <ProcessingDate>2017-11-22</ProcessingDate>--处理日期
      <SampleNumber>LF0111</SampleNumber>--样品编号
      <BarCodeNumber>0300679931</BarCodeNumber>--条码编号
      <EncompassingEncounterType>门诊</Encompassing-
        EncounterType>--就诊类型
      <PatientId>A101496681</PatientId>--患者唯一标识码
      <PatientName>李保贵</PatientName>--患者姓名
      <PatientSex>男</PatientName>--患者性别
      <PatientAge>63 岁</PatientName>--患者年龄
      <CostCategory>自费</CostCategory>--费用类别
      <SpecimenSpecies>血</SpecimenSpecies>--标本种类
      <ApplicationDepartment>肿瘤内科门诊
      </ApplicationDepartment>--申请科室
      <ApplicationWard>XXXXXX</ApplicationWard>--申请病区
      <BedNum>XXXXXX</BedNum>--床号
      <ApplicationDoctor>徐志宏</ApplyDoctor>--申请医生
      <Diagnosis>XXXXXX</Diagnosis>--诊断
      <Remarks>申请采集：B0203...</Remarks>--备注
      <Rapporteur>吕伟华</Rapporteur>--报告人
      <Proofreader>韩旺</Proofreader>--校对人员
      <ApplicationTime>2017-11-22 08:45</ApplicationTime>--申请时间
      <SamplingDate>2017-11-22 09:15</SamplingDate>--采样时间
    </ClinicalBaseDocElement>
    <!-- 具体诊疗内容 -->
    <EncompassingEncounterContent>--cxhw|1|A101496681|李保贵|1|63 岁
|1482|A010901|2017-11-22 11:07|1|APTT， 28.20|APTT-R， 0.81|AT-III，
88.00|D-DIMER， 0.333|FIB， 6.73|INR， 1.27|PA， 65.0|PTR， 1.27|TT，
13.4|TT-R， 0.92|
    </EncompassingEncounterContent>

```

```
<!--数字签名数据关联路径-->
<Description
Xlink:type=" simple"
Xlink:href=" ../../Signature" >--数字签名数据存放路径
</Description>
</ClinicalDocumentElement>
```

附录 C 数字签名司法鉴定参考流程

（资料性附录）

医院进行医疗纠纷处理和司法诉讼过程中，需要证明经数字签名电子病历的真实性、完整性时，可通过电子数据司法鉴定中心对电子病历进行司法鉴定的方式，使之成为有效证据。

电子数据司法鉴定中心是指经国家批准成立的从事电子数据司法鉴定的专门机构，主要提供电子数据证据内容一致性的认定、对各类电子设备或存储介质所存储数据内容的认定、对各类电子设备或存储介质已删除数据内容的认定、加密文件数据内容的认定、计算机程序功能或系统状况的认定、电子数据证据的真伪及形成过程的认定等服务。

电子数据司法鉴定中心将依照《中华人民共和国电子签名法》中对数据电文证据法律效力的相关规定，针对使用数字签名系统实现数字签名的医院电子病历数据，经有权主体提出鉴定委托，开展鉴定工作，利用数字签名、校验分析和一致性比对等鉴定技术手段，对医院所提交的经数字签名的电子病历，以及签名相关的证明材料进行分析、鉴别，以判断相关电子病历数据是否被篡改及数字签名行为的真实性，并出具具有法律效力的鉴定技术报告。

数字签名司法鉴定的参考流程如图 C.1 所示。

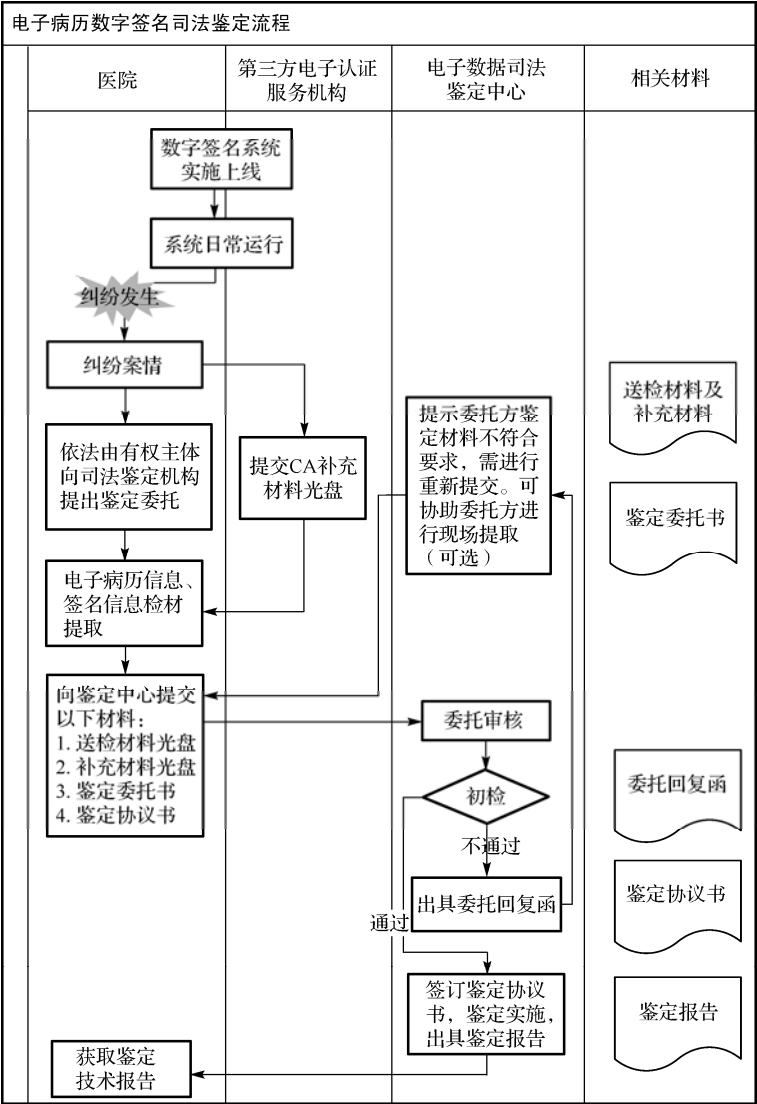


图 C.1 电子病历数字签名司法鉴定参考流程

附录 D 医院数字证书使用及管理

办法示例

（资料性附录）

第一条 为进一步规范我院数字证书的使用，依照《卫生系统电子认证服务规范（试行）》的要求，规范数字证书的管理，制定本办法。

第二条 本办法适用于我院内，办法中所称数字证书指个人数字证书。个人数字证书用于认证院内工作人员的身份。

第三条 为提高我院信息系统整体的身份认证强度，我院内部局域网各类应用系统原则上都要通过数字认证才能进行访问，启用数字证书的同时，即可停用传统的用户名、口令登录方式。

第四条 信息中心负责院内数字证书的统一管理，包括数字证书的办理、发放、注销和停用等。

第五条 院内用户的数字证书由信息中心统一申请，新调入人员若在原单位已申请数字证书，原则上不再重新申请数字，其证书在信息中心注册后即可使用；调出人员需将所持数字证书（UKEY）交回信息中心，如不交回按照丢失处理。

第六条 申请、吊销使用数字证书的单位（个人）

需填写相应表单，并确保信息的真实、准确、完整。领用数字证书时，相关人员需要在数字证书领用登记表上签字。

第七条 数字证书使用的有效期限为一年。有效期满一个月前登录应用系统时，系统会自动提醒用户更新证书并进行自动更新。当证书无法自动更新时，用户可根据相关说明携带数字证书（UKEY）到我院证书受理点（院信息中心）办理更新操作（无须更新存储介质）。

第八条 数字证书持有者应对其妥善保管，并对使用证书的行为负责，禁止将证书转借他人使用。

第九条 证书持有者应牢记数字证书介质的保护口令，如果连续多次尝试错误，证书介质将拒绝使用（称为“锁死”）。一旦发生锁死情况，请携带证书介质及初始密码卡到信息中心进行解锁。

第十条 发生下列情形之一的，数字证书持有人应及时向信息中心申请停用，否则将有可能被追究证书持有人的责任。

- （一）证书丢失；
- （二）证书中的姓名、身份证号等信息发生重大变更；
- （三）认为本人不能履行数字证书认证业务规则。

第十一条 发生下列情形之一的，信息中心可废止数字证书。

- （一）证书持有人申请废止数字证书；
- （二）证书持有人提供的信息不真实；
- （三）证书持有人没有履行双方合同规定的义务；
- （四）证书的安全性得不到保证；

（五）法律、行政法规规定的其他情形。

第十二条 发生介质损坏或丢失情况的，信息中心可重新签发数字证书。

第十三条 本办法由信息中心负责解释和修订，自发布之日起试行。

年 月 日

附录 E 医院数字证书及其介质管理

细则示例

（资料性附录）

以某医院数字证书及其介质（USB Key）管理规定为例。

1. 医务人员数字证书及其介质使用规定

（1）仅向具备我院执业资质的医务人员发放数字证书及其介质（USB Key）。

（2）我院具备执业资质的医务人员申请数字证书及其介质，需经科主任同意、医务处批准，并携带本人身份证去信息中心办理。由信息中心采集手写体签名图片，与身份证复印件一起存档。

（3）具有数字证书及其介质的医务人员应及时设立可靠的证书介质访问密码，并妥善保管。一旦发生故障或损坏，由信息中心负责维修和更换。丢失补办照价赔偿。

（4）数字证书及其介质仅限医务人员本人使用，不得将密码和相应权限授予他人，因上述行为导致的一切不良后果由该证书介质拥有者承担全部责任。

（5）无证书介质的工作人员和学生不得利用他人的证书介质从事病历书写和行使其他医疗行为。上述行为一经发现，按非法行医处理。

(6) 无我院执业资质的医务人员（进修医师、研究生、实习生）可以使用上级医师的附属账号登录病历系统创建草稿，但无提交、保存病历的权限，其签名只以印刷体出现在病历中。

(7) 医务人员在离开我院时，其数字证书及其介质由信息中心收回，并取消该证书介质的使用权。

(8) 信息中心确保证书介质的使用安全性，除本人使用外，防止其他途径的复制、模仿其签名功能等，保证其唯一性和安全性。

(9) 数字证书的有效期为一年，过期后由信息中心重新签发。

2. 患方电子签名规定

(1) 为进一步实现电子病历无纸化，各类知情同意书、签字病程等需由患者或家属签字的文书使用事件性数字证书进行数字签名。

(2) 所有患方数字签名必须同时具备患者或家属的数字签名和指纹认证，二者缺一不可。

(3) 对于无能力完成签名的患者，可由患者家属代替完成签名，并采集患者指纹。

3. 数字证书管理制度

数字证书的业务管理包括数字证书初次办理，数字证书更新，数字证书信息变更，证书介质丢失补办、损坏补办，证书介质解锁，数字证书吊销。

1) 数字证书初次办理

(1) 定义：用户第一次申请办理数字证书，称为初

次办理。

(2) 用户需提交的资料：填写好的一式两份《个人数字证书申请表》，科主任和医务处签字；申请人身份证原件和复印件；办理人身份证原件。

(3) 数字证书的有效期为一年；

(4) 管理员通过系统操作办理数字证书。

2) 数字证书更新

数字证书的有效期为一年，到期后需要进行证书更新。

数字证书更新的流程如下。

(1) 用户向受理点提出更新申请，受理点负责验证用户的真实身份（提交材料与初次办理一致）。

(2) 受理点制证员与第三方电子认证服务机构管理员联系，管理员核实了信息后为用户进行网上更新授权。

(3) 用户登录“医院单点登录系统”，进行证书下载更新。

3) 数字证书信息变更

(1) 定义：用户证书在有效期内，出现基本信息变更（姓名），需要执行证书信息变更操作。

(2) 需要提交的资料：填写好的一式两份《个人数字证书申请表》，科主任和医务处签字；变更后的申请人身份证原件和复印件；经办人身份证原件；原证书介质 USB Key。

(3) 用户信息变更，证书原有效截止日期不变。

(4) 管理员通过系统操作进行数字证书信息变更。

4) 证书介质丢失补办、损坏补办

(1) 定义：用户证书介质在有效期内发生丢失、损

坏的情况，用户需申请办理补办业务。

（2）证书介质丢失需去财务处缴费后到信息中心补办，证书介质损坏的直接到信息中心办理更换。

（3）用户需提交的资料：证书介质丢失补办，需提交由财务处盖章的“智能卡申请办理缴费单”。

（4）为保证安全，在进行证书丢失补办、损坏补办业务的同时，系统会自动吊销那张丢失、损坏的证书。

（5）补办证书的有效截止日期不变。

（6）管理员通过系统操作办理。

5) 证书介质解锁

（1）锁死的原因：连续 10 次输错密码，导致证书访问密码锁死；用户忘记证书密码。

（2）需要提交的资料：填写好的一式两份《个人数字证书申请表》，科主任和医务处签字；申请人身份证原件和复印件；经办人身份证原件；原电子密钥 **USB Key**。

（3）解锁后，密码重置。

（4）证书原有效截止日期不变。

（5）管理员通过系统操作进行解锁。

6) 数字证书吊销

（1）定义：用户证书发生外泄时，用户已有证书需做吊销处理。

（2）用户需提交的资料：填写好的一式两份《个人数字证书申请表》，科主任和医务处签字；申请人身份证原件和复印件；办理人身份证原件。

（3）管理员通过系统操作进行吊销。

附录 F 名词解释

（资料性附录）

1. 数字证书 certificate

用于标识行为主体网络身份的一种数据，该数据由第三方电子认证服务机构的私钥签发，且无法伪造。

2. 电子病历 electronic medical record

本规范所称的电子病历是指医务人员在医疗活动过程中，使用医疗机构信息系统生成的文字、符号、图表、图形、数据、影像等数字化信息，并能实现存储、管理、传输和重现的医疗记录，是病历的一种记录形式，其中包括门（急）诊电子病历、住院电子病历。

3. 电子病历系统 electronic medical records system

本规范所称的电子病历系统是指医疗机构内部支持电子病历信息的采集、存储、访问和在线帮助，并围绕提高医疗质量、保障医疗安全、提高医疗效率而提供信息处理和智能化服务功能的计算机信息系统，既包括应用于门（急）诊、病房的临床信息系统，也包括检查检验、病理、影像、心电、超声等医技科室的信息系统。

4. 数字签名 electronic signature

是指符合《中华人民共和国电子签名法》规定并且含时间戳的可靠数字签名。

5. 数字签名服务系统 electronic signature service system

能够独立完成数字签名功能的服务系统。

6. 摘要 digital digest

是唯一对应一个消息或文本的固定长度的值，它由一个单向 Hash 加密函数对消息进行作用而产生。

7. 签名算法 signature algorithm

用来保证数字签名信息的安全，提供鉴别、完整性、抗抵赖等服务的加解密数学函数的集合。

8. SM 算法

椭圆曲线国产商用密码算法。为保障商用密码安全，国家商用密码管理办公室制定了一系列密码标准，包括 SM1、SM2、SM3、SM4、SM7、SM9、祖冲之密码算法等，并于 2011 年要求各类投入运行并使用公钥密码的信息系统及商用密码产品使用 SM2 椭圆曲线密码算法。

9. 时间戳 time stamp

是指基于权威可靠时间源的时间信息，对原始文件信息使用可靠数字签名技术产生的数据，签名对象包括原始文件信息、签名参数、签名时间等信息。

10. USB Key

USB Key 是一种 USB 接口的硬件设备，是一种硬件数字证书载体。它内置单片机或智能卡芯片，可以存储用户的私钥及数字证书，利用 USB Key 内置的公钥算法实现对用户身份的认证。

11. 哈希值 Hash

把任意长度的输入通过哈希算法变换成固定长度的输出，该输出就是哈希值。

12. PIN 码 Personal Identification Number

个人识别码是一种保护数字证书使用的安全措施。

参 考 文 献

- [1] 中华人民共和国电子签名法.
- [2] GB/T 25064—2010 信息安全技术 公钥基础设施 电子签名格式规范.
- [3] 病历书写基本规范（卫医政发〔2010〕11号）.
- [4] 卫生系统电子认证服务管理办法（试行）（卫办发〔2009〕125号）.
- [5] 卫生系统数字证书格式规范（试行）（卫办发〔2009〕125号）.
- [6] 卫生系统数字证书应用集成规范（试行）（卫办发〔2009〕125号）.
- [7] 电子病历系统功能规范（试行）（卫医政发〔2010〕114号）.
- [8] 电子病历应用管理规范（试行）（国卫办医发〔2017〕8号）.
- [9] 医疗机构病历管理规定（2013年版）（国卫医发〔2013〕31号）.

反侵权盗版声明

电子工业出版社依法对本作品享有专有出版权。任何未经权利人书面许可，复制、销售或通过信息网络传播本作品的行为；歪曲、篡改、剽窃本作品的行为，均违反《中华人民共和国著作权法》，其行为人应承担相应的民事责任和行政责任，构成犯罪的，将被依法追究刑事责任。

为了维护市场秩序，保护权利人的合法权益，我社将依法查处和打击侵权盗版的单位和个人。欢迎社会各界人士积极举报侵权盗版行为，本社将奖励举报有功人员，并保证举报人的信息不被泄露。

举报电话：(010) 88254396; (010) 88258888

传 真：(010) 88254397

E-mail: dbqq@phei.com.cn

通信地址：北京市万寿路 173 信箱

电子工业出版社总编办公室

邮 编：100036